Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 168

Files HC16-10-2 and HI16-17

London Health Sciences Centre

December 17, 2021

Summary: This decision addresses both an individual complaint and an IPC-initiated investigation into a hospital's practices around its agents' use of personal health information for education purposes. In the individual complaint, a hospital patient alleged that a doctor had improperly accessed her health records while claiming an education purpose for the accesses. The patient's allegations raised broader questions about whether the hospital had in place adequate information practices to govern this use of personal health information by its agents. The IPC opened the self-initiated investigation to address those systemic issues.

In this decision, the adjudicator finds there were a number of unauthorized accesses to the patient's health records. These accesses were made in violation of the hospital's policy on education use, which permits patients to refuse consent to this use, and the patient's withdrawal of consent under the policy. The adjudicator finds these accesses were violations of the *Personal Health Information Protection Act, 2004* (*PHIPA*). After considering the circumstances surrounding the accesses, she concludes they were largely the result of systemic deficiencies in the information practices around education use that the hospital had in place at the time. These were failures by the hospital to comply with its obligations under *PHIPA*, including its duty to take reasonable steps to protect personal health information in its custody or control.

The adjudicator then considers a number of changes the hospital has already made or has committed to making to its information practices in response to the breaches, as well as the hospital's cooperation throughout the IPC process. In view of all the circumstances, she finds it unnecessary to issue orders against the hospital. However, she provides guidance to the hospital in the form of three key recommendations, as well as some additional

recommendations, for further improvements to its information practices in relation to the use of personal health information for education purposes.

Statutes Considered: *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Sch A, sections 2 (definitions), 10(1) and (2), 12(1) and (2), 15(3)(b), 16(2), 17, 18, 19, 20(2), 29(a), 30, 37(1)(e), and 37(2).

Decisions Considered: Order HO-013; PHIPA Decisions 102, 110, and 144.

INTRODUCTION:

[1] This decision addresses the use of personal health information by health information custodians and their agents for the purpose of educating agents in relation to the provision of health care. These uses are common in the health care sector, and can include familiar examples like a medical student's accessing a patient chart in learning how to properly document the provision of care, and a discussion between hospital agents during a medical round about a patient's condition.

[2] The *Personal Health Information Protection Act, 2004* (*PHIPA*) recognizes that these are legitimate and appropriate uses of personal health information in some circumstances. However, as the facts below illustrate, these uses must be governed by a custodian's clearly articulated policies and procedures, which must be properly implemented and reinforced by regular training and audits. Effective information practices and implementation of those practices are necessary conditions to ensuring that a custodian's agents understand and comply with their duties, both under the custodian's information practices and under *PHIPA*.

[3] In this decision, I consider issues arising from a hospital patient's allegations that hospital agents improperly accessed her records of personal health information based on claims of education use. I examine these accesses in the context of the hospital's information practices governing its agents' use of personal health information for education purposes. These practices include the hospital's consent-based approach to education use, its procedures for implementing this consent-based approach, and its training for its agents. Ultimately, I find there were a number of unauthorized accesses to the patient's records, made in violation of the hospital's policy and of *PHIPA*.

[4] After considering all the circumstances, including the hospital's responses to the breaches, its cooperation throughout the complaint and investigation processes, and its willingness to respond to the guidance provided by this office, I decide it is unnecessary to issue orders against the hospital. However, I make a number of recommendations to the hospital to further improve its information practices governing this important use of personal health information by its agents.

BACKGROUND:

The first complaint (HC16-10), and the IPC-initiated file (HI16-17)

[5] A medical resident at the London Health Sciences Centre (the hospital) who was also a patient of the hospital believed that other medical residents were accessing her health records without authorization. She filed a complaint with the Office of the Information and Privacy Commissioner/Ontario (IPC) about her concerns.

[6] The IPC opened Complaint HC16-10 to address this matter. The hospital conducted an investigation of accesses by two particular residents whom the complainant suspected of inappropriately viewing her records. After its investigation, the hospital concluded that the residents' accesses had been made for education purposes, which was a permitted activity by the hospital. However, as a result of the complaint, and because it appeared to the hospital that it lacked clear guidelines on its agents' use of personal health information for education purposes, the hospital updated its policy titled "Use of Personal Health Information for Research, Education and Quality Assurance."

[7] The hospital provided the complainant with an opportunity to provide feedback on its updates to the policy, which included new references to a patient's right to withdraw her consent to the use of her information for education purposes. In addition, to address the complainant's specific concerns about her colleagues' accesses to her records, the hospital placed a "lock box" restricting access to the complainant's personal health information in hard copy and in its electronic health records system (EHR), over a defined time period requested by the complainant. As discussed below, the hospital describes the lock box as a consent directive that allows a patient to "lock" (prevent) hospital agents' access to the patient's health records.

[8] The IPC also opened IPC-initiated File HI16-17 to address systemic issues raised by the complaint. These include issues around the adequacy of the hospital's policies and procedures addressing the use of personal health information for education purposes, and the hospital's training of its agents on these policies and procedures.

[9] In view of these developments, the complainant agreed to close her individual complaint file HC16-10.

The second complaint (HC16-10-2)

[10] During the course of the IPC's investigation in File HI16-17, the complainant became concerned about new accesses by her colleagues to her EHR records, in violation of the hospital's updated policy and her consent directive.

[11] These new accesses occurred around the time the complainant was admitted to hospital on several occasions. On each admission, she informed hospital staff that she had withdrawn consent to the use of her personal health information for education

purposes, as permitted by the hospital's updated policy (meaning the policy the hospital had put into place to address some of the concerns raised by Complaint HC16-10). The complainant alleges that despite the hospital's updated policy and her withdrawal of consent, there was no documentation of her withdrawal of consent in the EHR, and that two of her colleagues (medical residents) continued to make unauthorized accesses into her records.

[12] The IPC opened new complaint HC16-10-2 to address the complainant's new allegations of unauthorized accesses to her health records. The hospital investigated these new accesses. It concluded that one of the two residents had accessed the complainant's records while providing health care to the complainant, and the complainant was satisfied with that explanation. However, the complainant continued to take issue with the accesses by the second medical resident (the doctor). This doctor had also made some of the accesses at issue in the complainant's first complaint to the IPC.

Mediation/investigation stages of Files HC16-10-2 and HI16-17

[13] Given the overlap in the issues, the IPC addressed Files HC16-10-2 and HI16-17 together at the mediation stage of the complaint file and the investigation stage of the IPC-initiated file. At these stages, an IPC mediator/investigator gathered information from the hospital about the hospital's investigation into the complainant's further allegations, and about broader changes the hospital had made to address systemic issues around the education use of patient records by residents and others at the hospital.[1]

[14] During the mediation stage of the new complaint, the hospital took the position that the doctor's accesses had been made for education purposes, which the hospital permits its agents to do. However, the hospital stated that these accesses violated the updated Education Use policy, which set out a general rule about the number of times a hospital agent could access a patient's records for education purposes. The hospital found that the doctor had exceeded this number of allowable accesses. The hospital stated that, as a consequence, the doctor's supervisor spoke to him about this violation of its policy, and placed a warning on the doctor's file.

[15] At this time, the hospital also advised the IPC that its EHR was not capable of documenting a patient's withdrawal of consent to the use of her personal health information for education purposes. As described in more detail below, the hospital explained that its procedure for implementing a withdrawal of consent was to discuss the withdrawal of consent with medical teams and to consult with its Privacy Office.

[16] Several months later, and while mediation of the new complaint was ongoing, the complainant again raised concerns about this doctor's accesses to her EHR records.

[1] None of the information that follows or that I considered in my review is subject to mediation privilege as described in section 57(2)(c) of *PHIPA*.

The complainant had been admitted to the hospital on four additional dates over a three-month period, and a log of accesses into her EHR records showed that the doctor had accessed her records on multiple dates during this same period.

[17] When asked by the IPC to address these additional accesses, the hospital newly asserted that its updated Education Use policy (which provided for the withdrawal of patient consent to education use) had not been in effect at the time of any of the doctor's accesses. In addition, the hospital did not provide a clear statement about whether it believed the doctor's accesses complied with *PHIPA*.

[18] However, the hospital described other measures that it had taken to address the complainant's ongoing concerns about her colleagues' accesses to her EHR records.

[19] One measure was the creation and implementation of a new warning pop-up (a "flag") in the complainant's records in the EHR, which informed all users who accessed the complainant's electronic records that based on the patient's request, her personal health information could be used only for patient care purposes, and not for secondary purposes such as education use. The hospital reported that after it applied the flag to the complainant's records in the EHR, there was a significant decrease in the number of users accessing her records. The hospital's audits also showed no further accesses into the complainant's EHR records by the doctor.

[20] As another measure, the hospital had a specialist in the relevant area direct medical residents in that area not to access the complainant's EHR records except for the provision of care. The specialist also spoke separately with the doctor about not using the complainant's personal health information for education purposes without her consent. In addition, the hospital endeavoured to continue monitoring accesses to the complainant's EHR records, and to keep her informed of its findings and measures to address her privacy concerns.

[21] Despite these developments, there remained a number of unresolved questions at the end of the mediation and investigation stages, including about which version of the hospital's Education Use policy was in effect at the time of the accesses at issue, and about whether, and when, hospital agents were made aware of the complainant's withdrawal of consent to the education use of her health records. In light of this, the two files were transferred to the adjudication stage of the process.

Adjudication of Files HC16-10-2 and HI16-17

[22] At the adjudication stage, I decided to conduct a joint review of both matters under sections 57(3) and 58(1) of *PHIPA*. Section 57(3) permits the IPC to review a complaint if it is satisfied there are reasonable grounds to do so. Section 58(1) permits the IPC to conduct a review of any matter, on its own initiative, where the IPC has reasonable grounds to believe that a person has contravened or is about to contravene a provision of *PHIPA* or its regulations. In this joint review, I considered the hospital's

information practices around education use—both those in effect at the time of the accesses at issue, and changes to those practices since that time—to decide, among other things, whether the hospital had taken reasonable steps to protect personal health information from unauthorized use, and whether the hospital adequately responded to the allegations of unauthorized use.

[23] In the discussion that follows, I find that some of the accesses at issue were made in spite of the complainant's withdrawal of consent under the hospital's consent-based approach to education use, and were thus unauthorized accesses under *PHIPA*. I explain my reasons for concluding that these unauthorized accesses, though made by the doctor, are largely attributable to systemic failures on the part of the hospital to take reasonable steps to protect personal health information in its custody or control. These include failures by the hospital to have in place effective information practices to implement its particular approach to education use, and to properly train its agents on its information practices. These were violations of the hospital's duties under sections 10, 12 and 17 of *PHIPA*, among others, and they contributed to multiple breaches of the complainant's privacy.

[24] I also consider the steps taken by the hospital to respond to the breaches, and to address some broader deficiencies in its information practices. These include the hospital's implementation of a new Education Use policy, and the more widespread adoption of a new flag in patient EHR records to indicate when patients have withheld or withdrawn their consent to education use of their personal health information. I also consider the guidance provided in this decision to the hospital and to other health information custodians regarding this common use of personal health information by the health sector.

[25] In view of all the circumstances, including the hospital's responses to the breaches and its cooperation throughout the IPC process, I find it unnecessary to issue orders against the hospital. However, I provide guidance to the hospital for further improvements to its information practices with respect to this important use of personal health information. As will be seen below, this guidance takes the form of three key recommendations to the hospital, aimed at clarifying the hospital's and agents' duties under *PHIPA*. I also make some additional recommendations to the hospital for amendments to specific information practices. My recommendations, and my reasons for them, appear throughout the discussion that follows, and are reiterated at the end of this decision for ease of reference.

DISCUSSION:

[26] I begin by outlining some of the relevant obligations of a custodian and its agents under *PHIPA* when a custodian permits its agents to use personal health information for education purposes. I then consider how these obligations apply in the circumstances of the accesses at issue, to decide whether these accesses were made in

violation of *PHIPA*, and the roles of the hospital and its agents in these accesses.

The relevant provisions of *PHIPA*

[27] It is not in dispute that the person who operates the hospital is a "health information custodian," and that the health records of patients (including the complainant's records at issue in this decision) are records of those patients' "personal health information," as those terms are defined in sections 3 and 4 of *PHIPA*. The personal health information in these records is in the custody or control of the hospital.

[28] This means, among other things, that the hospital must comply with *PHIPA*'s rules concerning the collection, use, and disclosure of the personal health information in its custody or control. These rules protect the confidentiality of personal health information and the privacy of individuals, while facilitating the effective provision of health care. One of the ways in which *PHIPA* achieves these purposes 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 *PHIPA* permits or requires these actions to be taken without consent (section 29).

[29] Accessing a patient's records of personal health information is a "use" of that information within the meaning of *PHIPA* (section 2).[2]

[30] *PHIPA* permits health information custodians (and their agents) to use personal health information *without* consent "for educating agents to provide health care" [sections 37(1)(e) and 37(2)].[3] However, as I discuss in more detail below, the hospital has adopted an approach to education use that is based on patient consent. This approach places certain obligations on the hospital and its agents, such as the need to ensure the validity of a patient's consent to such uses, and to effectively document and implement a patient's refusal of consent.

[31] Custodians must take reasonable steps to protect personal health information in their custody or control, including against unauthorized use [section 12(1)]. The duty to take reasonable steps to protect personal health information 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.[4]

[32] A related obligation is the duty for custodians to have in place and to comply with information practices, which are the custodian's policy for actions in relation to personal health information, including:

---

[2] The definition of "use" in *PHIPA* was amended during the time period covered by the complaint, but the amendment has no impact on my review.

[3] "Agent" and "health care" are defined terms in *PHIPA* (section 2). A health information custodian that is permitted to use personal health information under section 37(1) may provide the information to an agent to use, for the same purpose, on the custodian's behalf [section 37(2)], and the providing of this information is a use, not a disclosure under *PHIPA* [section 6(1)].

[4] PHIPA Decision 44, at para 140. See also PHIPA Decisions 74, 80, and 110, among others.

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 [sections 2, 10(1) and 10(2)].

[33] Custodians must take reasonable steps to ensure that their agents are aware of and understand their obligations under *PHIPA* and under the custodian's information practices.[5] Agents act on behalf of the custodian, and not for their own purposes, in relation to personal health information in the custodian's custody or control. It is not in dispute that the doctor whose accesses are discussed in this review was at all relevant times an agent of the hospital.

[34] Section 17 of *PHIPA* addresses, among other things, the conditions under which a custodian may permit its agents to use personal health information, on the custodian's behalf, in the course of the agents' duties. Section 17 also provides that the custodian remains responsible for the information handled by its agents [sections 17(1) and 17(3)(b)], and may impose conditions or restrictions on its agents' handling of personal health information on its behalf [section 17(1.1)].[6] A violation of such conditions or restrictions is itself a violation of *PHIPA*.[7]

[35] In addition, section 30 of *PHIPA* sets out a limitation principle that is generally applicable to any collection, use or disclosure of personal health information. The relevant provisions require custodians to use no more personal health information than is reasonably necessary to meet the purpose of the use, and not to use personal health information at all, if other information that is not personal health information would serve the purpose.

Did the hospital take steps that were reasonable in the circumstances to protect the complainant's personal health information from unauthorized access?

[36] With the above background in mind, I now turn to considering the circumstances of the accesses at issue in this review. I examine the hospital's information practices governing education use that were in effect at the time of these accesses, to understand the context in which the accesses occurred, and to decide whether they were made in violation of *PHIPA*. I also consider some changes the hospital has made to its information practices since that time, in response to the complainant's allegations.

---

[5] Sections 12(1), 15(3)(b), and 17. While some of the accesses at issue in this review pre-date the coming into force of amendments to section 17, these amendments have no effect on the issues under review.

[6] These references are to the current version of section 17. See note 5, above.

[7] Sections 10(2) and 17(4)(a). Also see PHIPA Decision 110, paragraph 78.

[37] In the discussion that follows, I conclude that there were a number of unauthorized accesses to the complainant's health records, and that these accesses were largely a result of the hospital's failure to take reasonable steps to protect personal health information from unauthorized use. This violation of the hospital's duty under section 12(1) of *PHIPA* encompasses failures by the hospital to have in place and to comply with appropriate information practices [as required by sections 10(1) and (2)], and to ensure appropriate oversight of its agents' handling of personal health information on the hospital's behalf (as required by sections 15(3)(b) and 17).

[38] I begin by considering the hospital's consent-based approach to the use of personal health information for education purposes, which is a key backdrop to the accesses under review.

The hospital is generally entitled to rely on patient consent for the use of personal health information for education purposes

[39] As noted above, *PHIPA* permits custodians and their agents to use personal health information for education purposes without consent (provided other relevant requirements of *PHIPA* are met). By contrast, the hospital has adopted an approach to education use that is based on patient consent. This consent-based approach is reflected in the relevant hospital policy and procedures, which are discussed in more detail under the appropriate headings, below. The hospital thus relies on section 29(a) of *PHIPA*, which provides for the collection, use, or disclosure of personal health information on the basis of an individual's consent.[8]

[40] Consent under *PHIPA* may be express or implied. These are not defined terms in *PHIPA*. An express consent is a consent that an individual gives in some clear and unmistakable fashion—for example, by saying "yes," or by signing a document. Express consent may be given orally or in writing. By contrast, implied consent to the collection, use, or disclosure of personal health information is a consent that a custodian may conclude has been given in particular circumstances, based on the actions or omissions of the individual.[9] For example, when a patient answers questions on a hospital survey and returns it to the hospital, it is generally reasonable for the hospital to infer that it has the patient's consent to collect that information from the patient.

[41] Except in certain circumstances in which consent must be given expressly (which do not apply here), *PHIPA* generally permits custodians to rely on implied consent for

---

[8] Section 29(a) also requires that the collection, use, or disclosure be (to the best of the custodian's knowledge) necessary for a lawful purpose. Given that educating agents to provide health care is a permitted use without consent in *PHIPA* [section 37(1)(e)], I find it reasonable to conclude that this same purpose qualifies as a "lawful purpose" within the meaning of section 29(a).

[9] Halyna Perun et al., *Guide to the Ontario Personal Health Information Protection Act* (Toronto: Irwin Law Inc., 2005), at pages 205-207. See also IPC, *Frequently Asked Questions – Personal Health Information Protection Act* (September 2015), at pages 16-18. Available online here: https://www.ipc.on.ca/wp-content/uploads/Resources/phipa-faq.pdf.

the collection, use, or disclosure of personal health information, provided the conditions for a valid consent are met. The conditions for a valid consent (whether express or implied) are set out in section 18 of *PHIPA*. They include the requirements that the consent relate to the particular information at issue, and that the consent be "knowledgeable."

[42] For a consent to be knowledgeable, it must be reasonable in the circumstances to believe that the individual knows the purposes of the collection, use, or disclosure at issue, and that the individual may give or withhold her consent [section 18(5)]. Unless it is not reasonable in the circumstances, a custodian's notice that describes the purposes of the collection, use, or disclosure, and which is made available where it is likely to come to the individual's attention, is a means of fulfilling this element of knowledgeable consent [section 18(6)].

[43] The IPC asked the hospital to explain how the requirements for a valid consent are met when a hospital agent uses patient personal health information for education purposes.

[44] The hospital states that as an academic teaching hospital, part of its mandate is the education and training of medical residents. The hospital proposes that because of this mandate, "large teams of clinicians can be within the circle of care, in part, for education and/or training purposes." The hospital also suggests that its patients are aware upon entering an academic teaching hospital that their personal health information will be used for education purposes. These are claims that the hospital has the implied consent of patients for the education use of their personal health information, based on the hospital's teaching mandate. These claims require closer inspection.

[45] While the phrase "circle of care" is not a defined term in *PHIPA*, it is commonly used to describe the conditions under which *PHIPA* permits some health information custodians to assume an individual's implied consent to the collection, use, or disclosure of personal health information for the purposes of providing health care or assisting in providing health care to the individual [section 20(2)].[10] It is clear from the text of section 20(2) that custodians who are entitled to assume a patient's implied consent may do so only for the purposes of providing *health care*, and not for other purposes, such as education purposes. On this basis, I reject the hospital's claim that assumed implied consent can apply to the use of a patient's personal health information for education purposes.

[46] Aside from assumed implied consent within the "circle of care," custodians may rely on implied consent to use personal health information in some circumstances [sections 18(2) and (3)]. Custodians relying on implied consent must ensure (and

[10] Custodians who rely on assumed implied consent to collect, use, or disclose personal health information for health care purposes must also comply with other applicable requirements in *PHIPA*, such as the limitation principle in section 30.

cannot assume) that all the required elements of consent are fulfilled. In order for the hospital to rely on patients' implied consent as the basis for using their personal health information for education purposes, it must be reasonable in the circumstances to believe that the patients know that their information will be used for this purpose, and that they may give or withhold their consent to this use [section 18(5)], among other requirements. The hospital provided the following evidence for its claim that these conditions are met.

[47] First, the hospital proposes that its role as an academic teaching hospital means that patients consent to the education use of their personal health information upon entry to the hospital. I am not convinced that incoming patients are generally aware of the hospital's status as a teaching hospital so that it is reasonable to infer their consent to this use based simply on the fact they present themselves to the hospital for health care.

[48] More persuasive is the hospital's evidence that it provides notice to its patients about the education use of their personal health information (among other uses). The hospital explains that this notice is given in the form of privacy posters and pamphlets that are made available throughout the hospital, including in patient units, clinics, and outpatient areas (such as cafeterias, waiting rooms, and hallways). The hospital provided the IPC with copies of these materials.

[49] Among other things, these materials inform patients about the types of information that the hospital typically collects from patients, the hospital's obligation to protect their information under Ontario law, and the patients' rights to access and to request corrections to their information. Most relevant to this review, these materials list the specific uses to which the hospital may put their information: In addition to the provision of care, these include secondary uses like "for teaching to educate health providers and students." The notices inform patients that they "will be asked for specific consent" in other circumstances, such as "to share your information with those not involved in your health care, e.g. lawyers, insurance companies, etc.," referring to *PHIPA*'s requirement that consent be express, and not implied, in certain circumstances.[11]

[50] The hospital's notices also state that patients may restrict some of the ways in which the hospital uses their information, and they advise interested patients to contact the hospital's Privacy Office. They also inform patients of their right to complain to the IPC if they are not satisfied with the outcome of a complaint made to the hospital's Privacy Office. The hospital's notices are simple to read and to understand, to the benefit of patients and members of the public who want to know how the hospital collects, uses, and discloses patient information, and how it protects the confidentiality

[11] Section 18(3) of *PHIPA*. This section of *PHIPA* addresses consent for the "disclosure" (rather than for the "use") of personal health information (as those terms are defined in *PHIPA*). However, in the context of the hospital's plain-language notices, I find no issue in the hospital's addressing disclosures as well as uses of personal health information in this section of its notices.

of this information and the privacy of its patients.

[51] Based on the evidence, I am satisfied that the hospital's privacy posters and brochures are posted in common areas or are otherwise made readily available to patients. I am also satisfied that these notices inform patients both that the hospital may use their personal health information for education purposes, and that patients may withhold their consent to these uses, and in this way fulfil the requirements of knowledgeable consent. I also accept that the other elements of a valid consent in section 18(1) are generally met when the hospital uses (and permits its agents to use) patient information for education purposes on the basis of consent.

[52] As a result, I accept that the hospital may generally use personal health information for education purposes on the basis of patient consent. In adopting this consent-based approach to education use, the hospital has imposed conditions on its agents' use of personal health information for this purpose that go beyond the explicit requirements of *PHIPA*, as the hospital is entitled to do under *PHIPA*.

[53] This does not end the matter, however. Having adopted a consent-based information practice relating to the use of personal health information for education purposes, the hospital and its agents were required to comply with this practice [section 10(2)]. The hospital was also required to ensure that this information practice was sufficiently clear so that it could be interpreted and applied by its agents (sections 15(3)(b) and 17). These obligations are part of the hospital's duty to take reasonable steps to protect personal health information in its custody or control, including from unauthorized use [section 12(1)].

[54] It is therefore necessary to examine how the hospital implemented its consent-based approach to education use in practice. Under the next headings, I will consider the hospital's Education Use policy and procedures, its training for agents, and its auditing and enforcement measures.

The Education Use Policy

[55] The hospital has in place a policy governing the use of patient information for education purposes. I will refer to this document as the Education Use policy, or the policy.[12]

[56] There are two versions of the policy that are relevant in this decision: the policy that was in effect at the time of all the accesses at issue in this review (which the hospital describes as the "updated" policy, for reasons discussed below); and the "current" policy, which incorporates changes to the updated policy and which remains

[12] While the policy covers other secondary (non–health care) uses of personal health information, those other uses are not at issue in this review, and I will not refer to those other portions of the policy in this decision.

the version of the policy in effect at the date of this decision.[13]

[57] At various stages of the IPC's process, the hospital provided the IPC with different versions of its Education Use policy, with conflicting information about which version was in effect at the time of the accesses complained of. For example, at one stage of the IPC's process, the hospital denied that the updated policy applied to any of the accesses under review. However, at the review stage, the hospital confirmed that the policy that was in effect at the time of all the accesses was the hospital's "updated" policy, by which the hospital means the version of the policy that it implemented to address the complainant's initial complaint HC16-10. As noted above, this updated policy contained a new reference to a patient's ability to refuse consent to the education use of her personal health information.

[58] The hospital's confusion about the version of the policy that was in effect at the time of the accesses likely contributed to the hospital's inconsistent position, during the mediation and investigation stages of these files, about whether the accesses at issue complied with the hospital's policy and with *PHIPA*. More significantly (and as described in more detail under a separate heading, below), it appears that hospital agents (including the doctor) were unaware at the time of at least some of the accesses that the updated policy was in effect.[14]

[59] Even assuming that the hospital's agents knew at the relevant times that the updated policy was the applicable version of the policy, this version contained a number of gaps and inconsistences around the policy's scope and the requirement for patient consent. The IPC brought several concerns about the updated policy to the hospital's attention during the mediation and investigation stages of these files, and the hospital responded, as follows.

[60] One significant issue with the updated policy (the policy in effect at the time of the accesses at issue) was a statement in the policy excluding from its scope any clinician's use of personal health information for education purposes. Because clinicians, as a group, would be expected to represent a significant category of hospital agents who use personal health information for education purposes, their exclusion from the policy was a major gap. The policy also employed, in various places, a number of different terms (among them "staff," "employees," "regulated health professionals," "affiliates," and "students"), which could create confusion about which hospital agents were covered by the policy and which were not.

[61] During the mediation and investigation stages of these files, the hospital agreed to amend its updated policy to make clear that clinicians are subject to the policy. The

[13] The "current" policy was made effective in October 2018. The hospital confirmed in November 2021 that the current policy remains in effect.

[14] This relates to issues with the adequacy of the notice and the training the hospital provided to its agents on the contents of the updated policy and the hospital's consent-based approach to education use. See the discussion under the heading "Privacy and confidentiality training," below.

hospital also confirmed that despite the different terms appearing in the policy, its Education Use policy applies to all agents of the hospital, and it agreed to standardize the terms appearing in the policy to make this clear. The hospital also agreed to apply definitions (including of the term "use") that are consistent with *PHIPA*.

[62] During the processing of these files, the hospital made these changes (and others that I describe below) to the updated policy. These changes are reflected in the hospital's current policy, which remains in effect today.

[63] During the earlier stages of the IPC process, the IPC also noted that some sections of the hospital's Education Use policy appear to apply only to hard copy records, and others only to EHR records. (This is the case both in the updated policy that was in effect at the time of the accesses under review, and in the hospital's current policy.) The hospital explained that one section of the policy applies only to paper records because such records are stored in the hospital's Health Records department, and agents must take some additional steps (like presenting in person with hospital ID) to access hard copy records for education purposes. The hospital confirmed, however, that other sections of the policy addressing education use are meant to apply to agents whether they use paper or electronic records.

[64] I am satisfied that the hospital recognizes that the requirements of *PHIPA* apply irrespective of the format of the records. The current policy contains a new statement advising that the Education Use policy applies to information regardless of its medium or storage location.

[65] I also want to acknowledge some additional revisions that the hospital made to its Education Use policy to address other issues raised by the IPC during the earlier stages of these files. These changes are reflected in the current version of the policy.

[66] These changes include: a specific prohibition against accessing for education purposes the health records of family, friends, celebrities, and VIPs to whom an agent has never directly provided health care (to replace the updated policy's permissive language); and clarification that the hospital requires its agents to seek approval from their relevant supervisors before (and not after) they access records for education purposes. (I discuss below the policy's specific requirements for obtaining such approval.) The current policy also tells supervisors to consider whether information that is not personal health information, or a lesser quantity of personal health information, would serve the educational purpose, which is a reference to the limitation principle in section 30 of *PHIPA*. In response to another suggestion, the hospital added to the current version of the Education Use policy a link to its policy for managing privacy breaches.

[67] I am satisfied that the hospital has incorporated into its current policy and procedures some of the privacy best practices it discussed with the IPC during the mediation and investigation stages of these files, and I do not need to address these

particular issues again in this decision.

[68] I now turn to a key question in this review, which is whether the hospital's Education Use policy adequately addresses the hospital's consent-based approach to its agents' use of personal health information for education purposes. I will consider both the updated policy and the current policy in this regard.

[69] For the reasons that follow, I conclude that at the time of the accesses at issue, the hospital failed to have in place an adequate policy, and in this way failed to meet its obligations under *PHIPA*. I also identify some deficiencies in the current policy, and make three key recommendations (as well as some additional recommendations) to address them.

[70] The hospital's Education Use policy (both the updated policy, and the current policy) requires in some circumstances that agents obtain express patient consent, sometimes in writing. For example, the policy requires that agents obtain express patient consent to use photographs, video or sound recordings for education purposes.

[71] The policy (both the updated policy, and the current policy) also places limits on whose personal health information agents may access for education purposes, and how often. The hospital explained that these rules were developed in consultation with the relevant hospital committee, based on what the committee determined was an appropriate number of accesses for education purposes.

[72] As one example, the policy provides that agents may access for education purpose the records of patients to whom they provided health care within the past year, and they may access such records only four times within this period. The policy appears to authorize accesses that meet these criteria without express consent on the part of the patient, although this is unclear from the policy itself. However, if an agent wishes to access a patient's records more than four times, and/or after one year after the agent last provided care to the patient, the policy requires the agent to obtain the patient's express, written consent.

[73] The updated policy (the one that was in effect at the time of the accesses at issue) also authorized education use of patient information in cases where an agent never provided health care to the patient, provided the agent obtained that patient's written consent. The current policy (the one in effect as of the date of this decision) removes this provision, meaning that agents can access for education purposes only the records of patients to whom they have provided health care; they cannot access for this purpose records of any patient to whom they have never provided care, even if they have that patient's consent.

[74] *PHIPA* itself does not contain these specific limits on when, or whose, personal health information may be used for education purposes. However, as noted above, a custodian may impose conditions or restrictions on its agents' handling of personal

health information on its behalf, and imposing such conditions or restrictions may be part of the custodian's response to its obligations under *PHIPA* to have and to comply with information practices, and to take reasonable steps to protect personal health information in its custody or control. *PHIPA* further specifies that agents must comply with any such conditions or restrictions imposed by the custodian [section 17(4)(a)]. Thus *PHIPA* makes clear that it is a contravention of *PHIPA* for an agent to contravene a custodian's rules governing its agents' handling of personal health information, including when those rules go beyond the specific requirements of *PHIPA*.

[75] This is an answer to the hospital's claim during this review that some of the accesses at issue in the complaint were a "breach of policy, not a breach of legislation," because the hospital's policy "imposes a higher standard" than *PHIPA*. The hospital thus suggests that in the case of a policy violation, other requirements of *PHIPA*, such as the duty under section 12(2) to notify the patient of the breach, would not apply.

[76] The hospital's interpretation is incorrect. Once the hospital imposes a condition or restriction on its agents' use of personal health information, it is not only the agents' responsibility to comply, it is also the hospital's responsibility to take reasonable steps to ensure its agents are aware of and comply with their responsibilities, both under the hospital's information practices and under *PHIPA*. The hospital also has notification duties under *PHIPA* in the event the hospital or its agents use personal health information in an unauthorized manner, including uses made without consent in a manner outside the scope of the description of its information practices [sections 12(2) and 16(2)].

[77] In view of the hospital's own confusion on this point, I make one of my key recommendations to the hospital. Specifically, I recommend that the hospital amend its information practices to clearly and consistently state that any use of patient information for education purposes in violation of the hospital's information practices is a violation of *PHIPA*, and can result in consequences under *PHIPA*, such as notification of the affected patient and a complaint to the IPC. (As noted, this recommendation and others I make throughout this discussion are reiterated at the end of this decision for ease of reference.)

[78] I next address another significant defect in the hospital's Education Use policy (both the updated policy in effect at the time of the accesses at issue, and the current policy). While the policy sets out certain scenarios in which express consent to education use is required, it is silent on the authority for education use in other cases. To address this gap, I make another key recommendation to the hospital. I recommend that the hospital amend its information practices to clearly and consistently state that the hospital's approach to the use of personal health information for education purposes is based on individual consent. This would require, among other things, that the hospital specify that the use of personal health information for this purpose is based on the implied consent of hospital patients (except in those cases where the hospital has decided to require express consent), and that, in the case of either implied or

express consent, patients can refuse consent (by withholding or withdrawing their consent) at any time to this use of their information.

[79] The policy should also contain information about the hospital's procedure for addressing patient refusals of consent to this use. One basic reason for including this information in the policy (and in the hospital's training) is to alert hospital agents to the existence of a standard procedure for documenting and implementing refusals of consent, and to clarify how agents are informed of a refusal of consent. I consider this procedure next.

Hospital's procedure for documenting and implementing a refusal (a withholding or withdrawal) of patient consent to education use

[80] Before any of the accesses at issue in this review, the complainant informed the hospital that she did not consent to hospital agents' use of her health records for education purposes. In addition, the hospital advised the complainant that placing a "lock box" on her EHR records would prevent its agents from accessing her records for education purposes, and she asked that this be done.[15]

[81] So, in this case, there were two different ways in which the complainant signalled to the hospital that she did not want her records accessed for education purposes. The complainant took the additional step of informing all hospital agents she encountered at the hospital (whenever she was admitted as a patient of the hospital) about her withdrawal of consent to the education use of her information.

[82] Nonetheless, it is clear that the doctor accessed the complainant's records a number of times, indicating an education purpose for several of these accesses,[16] after the complainant had withdrawn her consent to such uses. The complainant also reported that none of the hospital agents she encountered seemed to be aware of her withdrawal of consent.

[83] During the review, I asked the hospital to describe the procedures that were in place at the time of the accesses to document and implement a patient's withholding or withdrawal of consent to the education use of her information. I also asked the hospital to describe any updates to its procedures since that time.

[84] Except as indicated below, the hospital's current procedures are the same as those that were in effect at the time of the accesses at issue.

[85] The hospital states that as a matter of general practice and policy, a patient's

---

[15] The term "lock box" is generally used to refer to consent directives preventing the collection, use, or disclosure of personal health care information for health care purposes (and not for secondary purposes such as education use). As seen below, it does not appear that the complainant intended, by requesting the lock box, to prevent accesses to her records for health care purposes.

[16] The hospital submits that other accesses by the doctor were made for the purpose of providing health care to the complainant, and thus were appropriate accesses under *PHIPA*. See also footnote 22, below.

refusal of consent to the education use of her information is to be documented on the patient's chart. However, the hospital's representations make clear that documentation on the patient's chart is not always possible.

[86] In the case of hard copy (paper) records, the hospital confirms that a refusal of consent to education use is documented directly in the patient's paper file. The patient's withholding or withdrawal of consent is also noted on a spreadsheet that is managed by the hospital's Privacy Office and its Health Information Management department, which department is responsible for providing hard copy records to an agent who asks to use them for education purposes. This department checks the spreadsheet before releasing any hard copy records for that purpose.

[87] For records in electronic format (EHR records), the hospital states that there is "no area in the EHR to document" a patient's withholding or withdrawal of consent for education use. Instead, the hospital explains, an agent who receives a refusal request is to contact the hospital's Privacy Office for direction on how to handle the request, and the Privacy Office is to "discuss the patient request with the relevant teams (medical, nursing, etc.) and work to develop a plan that is unique to the situation." The hospital states that its Privacy Office and the Health Information Management department work together to document these requests on a spreadsheet.

[88] Other than documenting on the spreadsheet, it appears the hospital has no defined procedure in place to deal with a patient's withholding or withdrawal of consent in the context of EHR records. The hospital's procedure is to "develop a plan." This may allow for greater flexibility to address unique situations, but it is not difficult to imagine how this method could lead to inconsistencies in the way the hospital manages refusals of consent. It also leaves agents without a clear picture of what to do and what to expect when a patient withholds or withdraws consent to the education use of her EHR records.

[89] The IPC has recognized that *PHIPA* does not specify how a custodian should implement a refusal of consent. For instance, in the context of a lock box request (which is typically understood to mean a withholding or withdrawal of consent in relation to collections, uses, or disclosures for health care purposes), the IPC has noted that custodians may comply through a variety of means, including policies, procedures or manual processes, electronic or technological means, or a combination of these.[17] The IPC has also recognized that there may be functional limitations in the technology used by a custodian; however, this does not relieve the custodian from its obligation to comply with *PHIPA*.[18]

[90] In this case, the hospital's EHR system does not allow it to document a patient's

---

[17] IPC Fact Sheet Number 8, "Lock-box Fact Sheet" (July 2005). Available online here: https://www.ipc.on.ca/wp-content/uploads/Resources/fact-08-e.pdf. See also PHIPA Decisions 102 and 144.

[18] PHIPA Decisions 102 and 144.

refusal of consent to education use directly in the patient's EHR records. (This was also the case at the time of the accesses under review.) While the hospital documents refusals of consent on a spreadsheet, this method is obviously more useful for preventing unauthorized uses in the context of paper records (since the relevant department checks the spreadsheet before giving paper records to an agent for education use) than it is for electronic records, which agents can access without this additional check.[19] This means the hospital must take other steps to ensure that it effectively manages a patient's refusal of consent in the context of EHR records.

[91] In the case at hand, there is no dispute that the doctor accessed the complainant's EHR records, citing education purposes for some of these uses, after the complainant had advised the hospital that she did not want anyone to access her health records for these purposes. (There is no claim that the doctor inappropriately accessed her hard copy records.)

[92] These accesses were made in violation of the complainant's withdrawal of consent, under the hospital's consent-based approach to this use, and were violations of *PHIPA*. Though made by the doctor, I find these privacy breaches are largely attributable to the hospital's failure to comply with its duties under *PHIPA* to take reasonable steps to protect personal health information and to ensure its agents' compliance with its information practices and with *PHIPA*.[20] My reasons follow.

[93] I have already described a number of issues with the updated policy that was in effect at the time of the accesses. As noted above, these raise questions about whether, when, and what agents knew about the hospital's Education Use policy and its consent-based approach to education use.

[94] I also find the hospital failed to have in place an appropriate procedure for documenting and implementing a patient's refusal of consent under this consent-based approach to education use.

[95] Based on the information provided by the hospital, I will assume that the appropriate hospital departments documented the complainant's withdrawal of consent in the spreadsheet, and noted the withdrawal directly in the complainant's paper records, in accordance with the hospital's procedures.

[96] The hospital was aware, however, that its EHR system would not indicate to agents accessing the complainant's electronic records that she had withdrawn her consent to the education use of her records.

[97] I understand that as a way around this issue, the hospital proposed to the

---

[19] Agents must also seek approval before accessing records (whether hard copy or EHR records) for education purposes. I describe this process under the next heading, below.

[20] I note that hospital agents have their own obligations under *PHIPA* to comply with the hospital's information practices and with *PHIPA* [sections 17(2) and 17(4)].

complainant that she impose a lock box on her EHR records, because (the hospital said) the removal of access under its lock box would also prevent access for education purposes. At that time, the hospital was already accustomed to employing electronic warning flags in its EHR system to implement patient lock box requests (to prevent access for health care purposes).

[98] From the information before me, it is unclear at what point exactly the hospital implemented the standard lock box flag on the complainant's EHR records. Even assuming the hospital applied the flag before any of the accesses at issue, it does not appear that the flag advised agents that use of the complainant's records for education purposes was prohibited by the complainant's lock box request.[21]

[99] There is no evidence that before the accesses at issue, the hospital provided any information to its agents about the complainant's withdrawal of consent to the education use of her health records, or took any other steps to implement her withdrawal of consent. In this regard, the hospital failed to take reasonable steps to ensure its agents were aware of their obligation, under the hospital's information practices and *PHIPA*, not to access the complainant's health records for education purposes. (This issue also relates to the adequacy of the training the hospital provided to its agents, which I consider under a separate heading, below.)

[100] Then, once the hospital became aware (through the complainant) that the doctor had accessed the complainant's EHR records for education purposes, the hospital had the doctor's supervisor speak to him about the updated Education Use policy, and it placed a warning on his file. However, the evidence from the hospital is that this discussion and warning concerned the fact the doctor had exceeded the allowable number of accesses for education purposes (set out in the updated policy). The discussion and warning does not appear to have addressed the crucial fact that the complainant had withdrawn her consent to any education use of her records.

[101] Some time after the discussion and warning, the doctor made several additional accesses to the complainant's EHR records, which the complainant again brought to the attention of the hospital. During the review, the hospital took the position that this set of accesses was not made for education purposes, but rather for health care purposes.[22] However, after learning the complainant's concerns about this second set of

---

[21] I base this assumption on the improved language of the new flag (which I discuss below) that the hospital created and implemented as a response to the new complaint. The hospital did not provide the IPC with a copy of the initial lock box flag that it applied to the complainant's EHR records.

[22] In its representations during the review stage, the hospital provided reasons for this view. Among other evidence, the hospital referred to the doctor's rotation schedule on the dates of the accesses and the dates of the complainant's admissions to hospital. I acknowledge that the complainant questions the hospital's conclusion about some of these accesses. However, she does not claim that any health care uses violated her consent directive.

The evidence on the doctor's "health care" accesses is equivocal, and I accept the hospital's submission that given the passage of time between the accesses and the hospital's investigation based on the new allegations from the complainant, the hospital had incomplete information upon which to make a

accesses, the hospital had a specialist speak to all members of the medicine team to warn them against accessing the complainant's EHR records except for the provision of care. The hospital also reports that the specialist spoke separately with the doctor about not using the complainant's personal health information for education purposes without her consent.

[102] This appears to be the first, and only, occasion on which agents were made explicitly aware of the complainant's withdrawal of consent. While these measures may have helped to prevent further inappropriate accesses to the complainant's records, they were taken only after some inappropriate accesses had already occurred. Moreover, whether it occurred before or after the breaches at issue, having a specialist tell agents not to access a given patient's EHR records for education purposes is not, by itself, a reliable method of effecting a patient's refusal of consent. Among other reasons, relying on a one-time oral direction to agents assumes that agents will maintain a perfect recollection of the discussion, and it requires that all agents who might access patient records for this purpose be present for the discussion.

[103] Since the time of these accesses, the hospital has taken steps to improve its procedure for managing patient refusals of consent for education use in electronic records. Following the complaint about the second set of accesses, the hospital's Privacy and Information Technology group built a custom flag for the complainant, which advised anyone accessing her EHR records that they could be used only for patient care purposes and not for any secondary purposes—including, specifically, education purposes. As noted above, there was a significant decrease in the number of accesses to the complainant's records after the flag was applied to them.

[104] The hospital states that it is now able to add this type of customized flag to the EHR records of any patient who withholds or withdraws consent to the education use of her records. This is a positive development. The IPC has recognized that flags can act as effective visual warnings against unauthorized access to electronic records.[23] Flags remind agents immediately before any use of EHR records about a patient's refusal of consent, which is for obvious reasons a superior system to one that relies on agents and supervisors to remember which patients have refused consent, and for what purposes. Flags can thus serve a similar function in EHR records to the notations the hospital already makes in hard copy records. This ensures that a patient's ability to exercise her rights under *PHIPA* is not affected by the format in which her personal health information appears. Flags can also inform agents that any accesses beyond the

---

determination about the appropriateness of those accesses. For these reasons, and because hospital agents' use of patient information for education purposes is the focus of this review, I decline to make findings in this decision about these particular accesses by the doctor.

[23] See, for example, Orders HO-002, HO-013, and PHIPA Decisions 102 and 110. See also IPC, *Detecting and Deterring Unauthorized Access to Personal Health Information* (January 2015), at pages 15-16. Available online: https://www.ipc.on.ca/wp-content/uploads/Resources/Detect_Deter.pdf.
To be an effective component of a privacy protection program, flags must have appropriate content, and be properly implemented: see PHIPA Decision 144.

flag may be subject to an audit (which is a hospital practice I recommend, below), and in this way provide another deterrent against unauthorized use.

[105] During the review, the hospital committed to updating its policy and training to clarify the different methods of documenting and implementing a patient's refusal of consent in the context of paper and electronic records. The hospital should also make clear that patients may withhold or withdraw their consent at any time, and that they may reinstate their consent at any time.

Procedure for accessing records for education purposes

[106] Assuming a patient has not withheld or withdrawn consent to the use of the patient's personal health information for education purposes, the hospital's agents may access the patient's records for these purposes based on implied consent or express consent. In either case, the hospital says, its agents must obtain approval for this use from their supervisors (or "leaders"). To address a gap in its updated policy (which did not specify the timing of obtaining the approval), the hospital's current policy now clarifies that agents must seek this approval before (and not after) accessing records for education purposes.

[107] During the review, the hospital explained that in order to obtain approval, an agent must explain the education purpose, identify the records the agent intends to use for this purpose, and explain how the records are relevant to the agent's area of work or study. The hospital also explained that it permits this approval to be given orally or in writing.

[108] The current policy states that agents who want to use hard copy records for education purposes must submit a request form to the Health Information Management department, and that agents who want to use electronic records for these purposes must document the reason for access within the relevant EHR file. The hospital provided the IPC with copies of the hard copy records request form as well as its EHR documentation requirements for secondary uses (including education use). To access electronic records for education purposes, agents are required to indicate the purpose of the access (as "Education"), and list the authorizing supervisor's name.

[109] To promote consistency in its procedures across different record formats, and because it is a good check against unauthorized access, I recommend that the hospital amend its hard copy records request form to require that agents similarly identify the authorizing supervisor before being granted access to those records.

[110] During the review, the hospital also stated that, assuming technical feasibility, it would consider requiring agents who use EHR records to provide additional details about the educational purpose (in the space provided in the EHR) before accessing those records. The hospital should ensure that any additional documentation requirements are also applied to agents who access hard copy records, by amending

the hard copy records request form.

Privacy and confidentiality training provided to agents who use personal health information for education purposes

[111] The hospital's Education Use policy states that agents who need to use personal health information for secondary purposes must complete the relevant organization's privacy and confidentiality education program. (The policy that was in effect at the time of the accesses at issue is identical to the current policy in this respect.) The IPC asked the hospital for details of the training that was provided to agents at the time of the accesses under review, and any updates to its training since that time.

[112] Except as indicated below, the training currently provided to agents is the same as the training that was in effect at the time of the accesses at issue.

[113] The hospital states that physicians and residents who work at the hospital and/or at St. Joseph's Health Care are "employed" by Western University, and receive privacy and confidentiality training at one of the two hospitals, where they are considered affiliates to the hospitals. The hospitals align their training and privacy policies to ensure consistency, as many physicians work at both hospitals.

[114] The hospital described for the IPC the various elements of its privacy and confidentiality training for its agents. The relevant training provided to physicians and residents includes: privacy training during orientation upon hire; a privacy component of the annual credentialing process for physicians; privacy and confidentiality "boot camps" for medical students and residents (which include presentations and teaching sessions) conducted about four times a year, with tracked attendance; and mandatory annual online privacy training (iLearn), completion of which is tracked.

[115] These training materials provide agents with a high-level introduction to *PHIPA* and various privacy issues they may encounter in their practice, such as examples of common privacy breaches and best practices to help avoid them. The training materials that were in place at the time of the accesses at issue also outlined some consequences of privacy breaches, including reputational harms to the hospital, and, for the agent, disciplinary action that could include a written warning, suspension, or termination of employment. I note that these consequences of a failure to comply are also set out in the current version of the hospital's Education Use policy, which states in addition that the hospital may report the agent to the agent's health regulatory college, where applicable.[24] This aligns with the IPC's advice that custodians should make their agents aware of the consequences of privacy breaches, as another deterrent against unauthorized activity.[25]

---

[24] In reference to *PHIPA* section 17.1.

[25] IPC, *Detecting and Deterring Unauthorized Access to Personal Health Information*, cited above. Seealso PHIPA Decisions 64, 80, and 102.

[116] During the IPC's review, the hospital acknowledged that at the time of the accesses at issue, its training materials informed agents that education use is a permitted secondary use of patient information, but did not explicitly state that the hospital's approach to this use is based on patient consent, or explain how this approach imposes additional conditions on education use beyond those set out in *PHIPA*.

[117] As I stated above, in relation to the hospital's Education Use policy, by failing to provide clear guidance to its agents about its particular approach to education use, the hospital failed to take reasonable steps to ensure its agents were aware of their obligations under the hospital's information practices and under *PHIPA*. This gap in the hospital's training of its agents, and the others that I describe below, are another way in which the hospital failed to comply with its duties under sections 12(1), 15(3)(b) and 17 of *PHIPA*.

[118] Based on her own experience, the complainant suggested during the review that the hospital include in the mandatory privacy training for its agents the most important elements of its Education Use policy. The hospital has since updated its training materials to address this topic, and it provided me with copies of those materials.

[119] These updated materials include specific examples in the annual online training and accompanying physician training to illustrate when agents may access patient records for education purposes, and what documentation is required before any access. The updated materials make clear that accesses for education purposes are subject to random or targeted audits to ensure compliance. The training directed at leaders also sets out the particular duty of those in supervisory roles to ensure that agents understand their obligations under the hospital's policies and *PHIPA*, and to monitor for compliance. Given the particular issues raised in these files, and more generally the commonness of education use in the health care sector, I agree with the complainant that the hospital should continue to include in its privacy training a component that specifically addresses its rules around education use.

[120] During the review, the hospital also committed to addressing a major gap in the oversight of its agents' training. The hospital explained that at the time of the accesses, it did not grant hospital staff access to its health information systems until they completed initial training and signed privacy and confidentiality agreements; however, the hospital did not apply this same practice to physicians and residents (who are not directly employed by the hospital).

[121] The hospital also advised that at the time of the accesses, the doctor had not completed any privacy training since his initial training as a medical student and resident, and was not in compliance with the hospital's training requirements. While the Medical Affairs department received notice of the doctor's failure to complete his annual training, and sent monthly notices to the doctor (in accordance with that department's practice), this did not impede the doctor's ability to access the hospital's patient

information systems, and ultimately to commit multiple breaches of the complainant's privacy.

[122] After the breaches at issue in this review, the hospital changed its practice to apply consistent requirements to all its agents, including physicians and residents. Now, a failure to complete annual privacy training results in the revocation of hospital privileges for physicians and residents, and all agents (including physicians and residents) must complete annual online training (after the initial training) in order to maintain their access to the EHR and other patient information systems. When hospital agents need to renew their privacy and confidentiality training, the relevant supervisor receives a notification. (The hospital reports that during this review process, the doctor completed his annual online privacy training, bringing him into compliance.)

[123] These changes to the hospital's training of its agents and oversight of that training will help to reduce the risks of unauthorized access by agents. The IPC has stated that regular and comprehensive privacy education and training of agents, and the use of confidentiality agreements (that are re-signed on a regular basis) are important tools to help reduce the risk of unauthorized access, and to foster a culture of privacy within an organization.[26]

[124] Also during the review, the IPC asked the hospital to explain how it informs its agents about any changes to its policies and practices. The IPC asked in particular how the hospital had informed its agents about the updated Education Use policy that was in effect at the time of the accesses at issue in this review. As noted, this updated policy contained a new reference to a patient's right to withdraw consent to the education use of her records, and was implemented in response to the complainant's first complaint to the IPC.

[125] The hospital explains that it typically informs medical affiliates of changes in hospital policies through electronic newsletters and newscasts called "e-casts." All agents also receive bi-weekly electronic communications from the hospital that include "privacy points." To announce the updated Education Use policy, the hospital says that it sent an e-cast to all agents six months after the policy's release. Because of changes to the hospital's email system since that time, the hospital was not able to confirm the exact date of the notice or to locate a copy of that e-cast; however, it believes the e-cast said that the hospital had updated its procedures around patient requests to restrict the use of personal health information, and around lockbox reversals and overrides.

[126] The failure to notify its agents of a relevant update to its policy for six months is another significant way in which the hospital failed in its duty under *PHIPA* to take reasonable steps to protect the personal health information of patients. Meeting this

[26] Among others, see Orders HO-010 and HO-013, and PHIPA Decisions 69, 102 and 110. See also IPC, *Detecting and Deterring Unauthorized Access to Personal Health Information*, cited above, at pages 12-15 and 16-17.

duty requires, among other things, that the hospital take reasonable steps to ensure its agents are aware at all times of the hospital's current information practices. To address this issue, I make my third key recommendation to the hospital. Specifically, I recommend that the hospital ensure it provides timely notice to its agents of any relevant changes to its information practices, such as updates to hospital policies and procedures. This means that when the hospital next revises its Education Use policy, in consideration of the guidance in this decision, the hospital should provide timely notification of the change to its agents.

Auditing and enforcement

[127] The hospital's Education Use policy (both the updated policy in effect at the time of the accesses at issue, and the current policy) states that audits are conducted to ensure compliance with the policy. The IPC asked the hospital for more details of its audits, including their nature and frequency, and whether audits are conducted on a random basis. As detailed below, the hospital's current practices with respect to auditing and enforcement are the same as those that were in place at the time of the accesses at issue.

[128] The hospital reports that all accesses to hard copy (paper) and electronic records are logged, and can be audited. In the complaint before me, there are no specific allegations of unauthorized accesses to paper records.

[129] Regarding audits of electronic records, the hospital explained that every access in a patient's EHR records is documented and logged, and can be subject to various standardized audits. Random audits of the different hospital systems containing personal health information occur on a scheduled basis. The electronic information system accessed for education purposes is subject to monthly random audits. Any agent with access to this system may be subject to a random audit. Audits are also conducted at the request of patients, or hospital supervisors who oversee hospital agents, and when major incidents (such as the admission of high-profile patients) occur. Audits can be conducted of particular patient records, or on particular users.

[130] The hospital says its agents are made aware of the hospital's audit processes at regular intervals, including as part of their privacy and confidentiality training at orientation and through the annual online training. The privacy and confidentiality agreements signed by agents advise them that their activities may be audited to ensure compliance; so does the Education Use policy itself (both the updated policy and the current policy). The hospital's corporate e-casts also include regular reminders about the hospital's auditing practices. All these messages are intended to discourage inappropriate accesses.

[131] I recommend that the hospital include a similar reminder about its auditing capabilities directly in the warning flags it places in the EHR records of patients who have refused consent in relation to their personal health information. A reminder in this

context, appearing immediately before a user gains access to any patient information, would be a clear and timely warning against unauthorized accesses.

[132] When the hospital conducts an audit (whether of electronic or hard copy records) and is unable to determine that an access was related to the provision of care (for example, because there is no documented reason for access, or the agent's call schedule does not suggest that the access was for the provision of care), the matter is forwarded to the appropriate leadership area and human resources. In the case of accesses by physicians and medical staff, the hospital's Medical Affairs department will investigate. The relevant department checks to see what reason, if any, the agent documented as the purpose for access. The hospital says that in the course of an audit, an access listed as an education use would prompt an assessment of the number of accesses for this purpose (because, as noted above, the hospital's policy sets a limit on the timing and number of accesses that an agent may make for education purposes on the basis of implied consent).

[133] However, as made evident during this review, there are also other factors that warrant special attention when examining accesses made for education purposes. These include whether the agent complied with all the documentation requirements before making the access, whether the patient whose records were accessed is someone with whom the agent has a personal connection, and whether the patient whose records were accessed has withheld or withdrawn consent to this use of the patient's records.

[134] During the review, the hospital noted that as a teaching hospital, it expects its agents (and especially medical residents) to access patient records for education purposes. However, the hospital says, this complaint and investigation process has highlighted for the hospital the importance of clearly communicating to its agents its expectations and rules around education use, and of carefully scrutinizing these accesses to ensure they are appropriate in the circumstances. The hospital says that it now routinely involves relevant supervisors in investigations by the Medical Affairs department into education accesses by physicians and residents that do not appear to comply with hospital policy or with *PHIPA*.

[135] The accesses at issue in this review were not detected through random audits, but as a result of the complaints filed by the complainant. Since then, as noted above, the hospital has developed customized warning flags that can be applied to the EHR records of patients who withhold or withdraw their consent to education use. If it does not do so already, the hospital should make a practice of routinely auditing accesses to records that are flagged in this way, and of notifying patients (and the IPC as necessary) about any unauthorized accesses, as required by *PHIPA*.[27] The hospital should also inform its agents (in its policy, training, and directly in the EHR flags) that it routinely audits accesses to flagged records.

[27] Sections 12(2) and (3), and section 16(2).

[136] Another of the complainant's concerns during this process was a lack of timely information from the hospital about its investigation of the accesses, and about any consequences to the doctor. The hospital has explained that it did not initially notify the complainant because it deemed the doctor's actions to be breaches of hospital policy, but not of *PHIPA*. This was a failure of the hospital's duty under section 12(1) to respond adequately to the complaint, as part of a proper response to the breach allegations, and to provide the complainant with the required notice under sections 12(2) and 16(2).

[137] Through this decision, the hospital is now aware that an agent's breach of the hospital's information practices is also a breach of *PHIPA*. In addition, during this review, the complainant received the hospital's representations, which contained the details noted in this decision about the hospital's response to her complaint, including its discussions with the doctor and the warning placed on the doctor's file. This accords with the IPC's past statements that an affected patient has the right to know not only the identity of the individual who breached her privacy, but also details of any disciplinary action taken, including the quantum of any penalty.[28] In the circumstances, I find it unnecessary to require the hospital to take further steps in respect of its notification obligations under *PHIPA*.

SUMMARY OF CONCLUSIONS

[138] I have concluded that at the time of the accesses at issue, the hospital failed to comply with its duty under *PHIPA* to take reasonable steps to protect its patients' personal health information. The breaches of the complainant's privacy that occurred were committed by the doctor, but I have found they are largely attributable to systemic failures on the part of the hospital to have in place and to ensure compliance with its information practices and with *PHIPA*.

[139] These failures encompassed deficiencies in the hospital's Education Use policy in effect at the time, a lack of adequate training and oversight of its agents in respect of this use, and an ineffective process for managing patient refusals of consent, despite the hospital's having adopted an approach to education use that depends wholly on patient consent. The matter before me is a clear example to show that a custodian's policy choices are effective only to the extent they are properly implemented.

[140] During the IPC process, the hospital made or committed to making changes to its information practices to address some of these deficiencies. I also took into account the hospital's demonstrated willingness throughout this process to respond to guidance from the IPC, to address both the specific breaches that occurred, and the broader systemic issues revealed by the complaint. In these circumstances, I found it unnecessary to issue orders against the hospital. However, throughout this decision

[28] IPC Orders HO-010 and HO-013.

(and as reiterated below), I have provided guidance to the hospital to further improve its information practices governing this important use of personal health information by its agents. This guidance takes the form of three key recommendations aimed at clarifying the hospital's and agents' duties under *PHIPA*, as well as some additional recommendations for amendments to specific information practices.

[141] Finally, I note that the IPC recommends that custodians revisit their privacy policies and procedures on a regular basis (at a minimum annually), and that these privacy policies and procedures specify the timing and other details associated with this procedure.[29] I so recommend here. The hospital indicated during the review that it reconsiders and revises its policies at regular intervals of about two years; however, as of the date of this decision, the hospital's current Education Use policy has been in effect for over three years. The hospital should revisit the policy as soon as possible, taking into consideration the guidance in this decision.

RECOMMENDATIONS:

For the foregoing reasons, pursuant to section 61(1)(i) of *PHIPA*, I make the following recommendations to the hospital:

KEY RECOMMENDATIONS

1. I recommend that the hospital amend its information practices to clearly and consistently state that the hospital's approach to the use of personal health information for education purposes is based on individual consent; that an individual may give, withhold, or withdraw consent, or reinstate consent, at any time; and that no education use is permitted where an individual has withheld or withdrawn consent.

2. I recommend that the hospital amend its information practices to clearly and consistently state that any use of personal health information for education purposes in violation of the hospital's information practices is a violation of *PHIPA*, and can result in consequences under *PHIPA*, such as notification of the affected individual and a complaint to the IPC.

3. I recommend that the hospital provide timely notice to its agents of any relevant updates to its information practices.

I make recommendations 1 and 2 in the context of the hospital's current, consent-based, approach to the use of personal health information for education purposes.

[29] *Detecting and Deterring Unauthorized Access to Personal Health Information*, cited above, at page 12.

These recommendations do not prevent the hospital from adopting a different approach in future to the use of personal health information for education purposes. In those circumstances, the hospital should amend its information practices accordingly.

ADDITIONAL RECOMMENDATIONS

I make the following additional recommendations for improvements to specific hospital practices:

Education Use Policy

4. I recommend that the hospital include details of the timing and procedure for future revisions to the Education Use policy (either directly in the policy itself or in a broader hospital policy).

5. I recommend that the Education Use policy:

    - include details of the hospital's procedure for documenting and implementing refusals of an individual's consent (including a withholding or withdrawal of consent) to the use of the individual's personal health information for education purposes; and

    - impose, to the extent possible, consistent approval and documentation requirements for the education use of hard copy (paper) and electronic records.

Auditing and enforcement

6. I recommend that the hospital routinely audit accesses made to records flagged in the EHR or in hard copy based on an individual's refusal of consent (including for the use of personal health information for education purposes).

7. I recommend that the hospital add to the EHR warning flags a notice about the hospital's auditing processes, including its routine auditing of accesses to flagged records.

8. I recommend that the hospital inform its agents about its auditing processes (including its routine auditing of accesses to flagged records), including in the Education Use policy and in its privacy and confidentiality training for agents.

Original Signed by: December 17, 2021

Jenny Ryu
Adjudicator