Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 176

Complaint HC19-00018

Windsor Regional Hospital - Ouellette Campus

April 5, 2022

Summary: This decision and related PHIPA Decision 177 address a complainant's allegations that a number of individuals at two hospitals made unauthorized accesses to records of his son's personal health information after his son's death. The records at issue in both decisions are contained in a shared electronic medical records system (EMR) accessible to both hospitals.

This decision addresses the allegations concerning accesses to EMR records in the custody or control of Windsor Regional Hospital – Ouellette Campus (WRH), as well as accesses by WRH agents to records in the custody or control of the other hospital, Hôtel-Dieu Grace Healthcare. In this decision, the adjudicator declines to consider the complaint against a WRH doctor in respect of two accesses in the EMR, because that matter has been appropriately dealt with in previous proceedings before the College of Physicians and Surgeons of Ontario. She finds that the remaining accesses were made in accordance with the *Personal Health Information Protection Act, 2004* (*PHIPA*), generally in relation to quality of care purposes permitted under *PHIPA*. She also finds that WRH generally complied with its obligations under *PHIPA* to take reasonable steps to protect personal health information in its custody or control, and to respond adequately to the complaint. As a result, she concludes the review without issuing an order. However, the adjudicator makes some comments and one recommendation to clarify WRH's obligations under *PHIPA* and to help improve its privacy practices in future.

Statutes Considered: *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Sch A (as amended), sections 2 (definitions), 3 (definition of "health information custodian"), 10(1) and (2), 12(1) and (2), 17, 29, 30, 36(1)(c)(iii), 36(1)(g), 37(1)(a), 37(1)(d), 37(2), 39(1)(d), and 57(4)(b); *Quality of Care Information Protection Act, 2016*, SO 2016, c 6, Sch 2.

Decisions Considered: PHIPA Decisions 80, 102, 110, and 168.

INTRODUCTION:

[1] This decision and related PHIPA Decision 177 address a complainant's allegations that a number of individuals made unauthorized accesses to records of a patient's personal health information after the patient's death. The complainant is the patient's father.

[2] The complainant filed complaints with the Information and Privacy Commissioner/Ontario (IPC) against two hospitals. One complaint (the one addressed in this decision) was made against Windsor Regional Hospital—Ouellette Campus (WRH). A related complaint was made against Hôtel-Dieu Grace Healthcare (HDGH). As I describe in more detail below, both hospitals provided care to the patient before his death, and at the relevant times shared an electronic medical records system.

[3] The IPC conducted separate reviews of the two complaints under the *Personal Health Information Protection Act*, *2004* (*PHIPA*). During the review stages of both complaints, the IPC sought and received representations on the issues from the hospitals and the complainant, which were shared between the parties in the relevant complaints in accordance with the IPC's *Code of Procedure for Matters under the Personal Health Information Protection Act, 2004*.

[4] The files were then transferred to me to continue the reviews. In the complaint against WRH, I notified an affected party (a doctor at WRH), who provided representations on the accesses alleged to have been made by him. I invited the complainant to respond to the affected party's representations, which he did. In addition, given the overlap in the parties and some of the accesses at issue in the two complaints, I shared relevant portions of WRH's and HDGH's representations with each other, and invited further responding representations from each hospital in the complaint against it. Both hospitals provided further representations, which I shared with the complainant. He provided comments in response.

[5] This decision addresses the allegations concerning accesses to patient records in the custody or control of WRH, as well as accesses by WRH agents to records in the custody or control of HDGH. (I discuss the meanings of the terms "agent" and "custody or control," below.) The related PHIPA Decision 177 addresses the allegations concerning accesses to patient records in the custody or control of HDGH, and the access by an HDGH agent to a record in the custody or control of WRH. Some of these accesses are addressed in both decisions, because of the overlap in the parties and the records at issue.

[6] In this decision, I decline to review aspects of the complaint that have been appropriately addressed in proceedings before the College of Physicians and Surgeons of Ontario. I find that the remaining accesses were made in accordance with *PHIPA*. I also find that WRH generally complied with its duties under *PHIPA* to take reasonable steps to protect personal health information in its custody or control. As a result, I dismiss the complaint. However, I make some comments and one recommendation to help improve WRH's privacy practices in future.

BACKGROUND:

[7] Before addressing the issues raised by the complaint, I will provide some background on the circumstances giving rise to the complaints against the two hospitals, the relationship between the hospitals, and the shared electronic medical records system containing the records at issue in both complaints. I will then describe the accesses at issue in the complaint against WRH.

The complaints

[8] The complainant provided the following information to place his complaints in context. The complainant's son (the patient) had received mental health care services at both WRH and HDGH. One day, the patient went to the WRH emergency department, and was released the same day. Several days later, the patient died by suicide.

[9] After the patient's death, because of concerns about the care the patient had received, the complainant asked WRH for a copy of the patient's medical records. He also asked WRH to conduct audits of accesses to the patient's records. These audits showed some accesses by individuals at both hospitals that the complainant believes were made for unauthorized purposes, in violation of the patient's privacy. For this reason, the complainant filed complaints with the IPC against both hospitals.

The shared electronic medical records system (Solcom)

[10] In the course of both complaints, WRH and HDGH provided useful background about the relationship between the two hospitals, which I summarize as follows.

[11] WRH and HDGH have a collaborative approach to the provision of health care in the Windsor-Essex area. Among other services, both hospitals provide mental health care in the region.

[12] The patient had received care from both WRH and HDGH. As a result, each hospital has in its custody and control records of the patient's personal health information that originate from the health care that each hospital provided to the patient. (As will be seen further below, a hospital with custody or control of personal health information has specific obligations under *PHIPA* in respect of that information.)

[13] In addition, during the time period of the accesses under review, WRH and HDGH had a shared electronic medical records system (EMR), called Solcom, for some patient records. While Solcom contained only a subset of each hospital's records, all the patient records at issue in this complaint and the related complaint were contained in Solcom.

[14] (Both hospitals retired Solcom after the time period covered by the complaints, for reasons unrelated to these complaints. WRH advises that WRH patient records are now contained in a new EMR called Cerner, which is accessible to users at both WRH

and HDGH. I discuss the new EMR later in this decision.)

[15] As I discuss in more detail below, WRH and HDGH both acknowledge that their duties and responsibilities in respect of the shared EMR are governed by *PHIPA*, as well as a data sharing agreement and each hospital's privacy policies. Among other things, each hospital acknowledges it has an independent responsibility under *PHIPA* (and under the agreement and policies) to protect the security of personal health information in the shared EMR.

The accesses at issue in this complaint

[16] This decision addresses the complainant's allegations that certain accesses to the patient's records in Solcom were made in contravention of *PHIPA*. To understand which records are at issue in the present complaint against WRH, it is helpful to set out some definitions here.

[17] While all the patient's records in Solcom were accessible to both hospitals, some of the records in Solcom originated from WRH (based on the patient's receiving care at WRH), while other records originated from HDGH (based on the patient's receiving care at HDGH). For ease of reference, in this decision I will refer to the former records as "WRH records," and the latter records as "HDGH records." This distinction is important, because it determines whether a given access in Solcom is a "collection," "use," or "disclosure" of the personal health information in the record by agents of each hospital involved in the access. (I elaborate on these terms further below.)

[18] At issue in the complaint against WRH are certain accesses to WRH records by individuals at WRH and HDGH. Also at issue are certain accesses to HDGH records by individuals at WRH.

[19] Specifically, the accesses at issue in this complaint are the following:

- Access #1 (occurring five days after the patient's death) by a doctor with privileges at WRH (whom I will describe in this decision as the "WRH doctor," or simply "doctor" where the context is clear), lasting approximately one and a half minutes. Access #1 was made to WRH records (a WRH emergency record and consultation note of the treating psychiatrist);

- Access #2 (occurring almost two years after the patient's death) by the WRH doctor, to the same records described in Access #1;

- Access by WRH Employee A (occurring six days after the patient's death) to various WRH records (emergency record, discharge summary, consultation note, and mental health form);

- Access by WRH Employee A (occurring the same day, six days after the patient's death) to various HDGH records (a clinic record, a clinic note, and a crisis note);

- Access by WRH Employee B (occurring several months after the patient's death) to various HDGH records;[1] and

- Access (occurring seven days after the patient's death) by a doctor with privileges at HDGH (the "HDGH doctor"), lasting approximately one minute, to a WRH record (a discharge summary).

[20] Some other accesses that were initially part of the complaint against WRH were addressed to the complainant's satisfaction during the mediation stage of the complaint, and are no longer at issue.

[21] In addition, the above-noted access by the HDGH doctor to a WRH record, and the accesses by WRH Employees A and B to HDGH records are also addressed in the related PHIPA Decision 177. This is because, as explained in more detail below, for each these accesses, there are two aspects of the transaction to be considered: the *collection* of personal health information by one hospital (through its agent); and the corresponding *disclosure* of that information by the other hospital (though its agent).

[22] For the reasons set out below, I decline to conduct a review of the complaint against the WRH doctor in respect of Accesses #1 and #2, because this issue has already been appropriately dealt with in proceedings before the College of Physicians and Surgeons of Ontario. (I do, however, separately address some broader issues raised by WRH's response to the complaint about the doctor.) I find that the remaining accesses to the patient's records were made in accordance with *PHIPA*. I also find that WRH complied with its duties under *PHIPA* to take reasonable steps to protect personal health information in its custody or control, and that it responded adequately to the complaint. I therefore dismiss the complaint against WRH. However, I make some comments and one recommendation to WRH to clarify its obligations under *PHIPA* and to help improve its privacy practices in future.

PRELIMINARY MATTERS:

[23] One of the purposes of *PHIPA* is to protect the confidentiality of personal health information and the privacy of the individuals to whom the information relates. *PHIPA* achieves this purpose by, among other things, requiring that all collections, uses, and disclosures of personal health information comply with *PHIPA*, and by imposing duties on health information custodians (and their agents) to take reasonable steps to protect personal health information in their custody or control.

[24] Before addressing the particular accesses at issue in the complaint, I make the following preliminary findings to confirm the application of *PHIPA* to the matters under review.

[1] For reasons I explain further below, it is not possible to identify which records were accessed by WRH Employee B on this date.

Health information custodians and agents

WRH and HDGH are health information custodians

WRH Employees A and B, the HDGH doctor, and the WRH doctor are agents of the relevant health information custodians

[25] There is no dispute, and I find, that WRH is a "health information custodian" within the meaning of *PHIPA* [paragraph 4.i of section 3(1)].[2] There is also no dispute in the related complaint against HDGH that HDGH is a health information custodian, and I find that it is. All the parties also agree that the records at issue in this complaint and the related complaint are records of the patient's "personal health information" within the meaning of *PHIPA* [section 4(1)]. As a result, *PHIPA*'s rules concerning the collection, use, and disclosure of personal health information apply to the handling of the patient's records by WRH and HDGH.

[26] These rules also apply to agents of WRH and HDGH. The term "agent" is defined in *PHIPA* to mean, generally, a person who, with the authorization of the custodian, acts for or on behalf of the custodian, and not for the agent's own purposes, in respect of personal health information (section 2). When a custodian permits an agent to act on its behalf in this way, both the custodian and the agent have responsibilities under *PHIPA* (section 17). *PHIPA* provides, among other things, that the custodian remains responsible for the information handled by its agent [sections 17(1) and 17(3)(b)].

[27] In this complaint there is no dispute that WRH Employees A and B were agents of WRH at the relevant times, and I find they were.

[28] There is also no dispute that the HDGH doctor was acting on behalf of HDGH, and not for his own purposes, in respect of his access at issue in this complaint. I find that the HDGH doctor was an agent of HDGH in respect of this access (section 3(3)1).[3]

[29] By contrast, WRH submits that the WRH doctor is not its agent in respect of Accesses #1 and #2. This is based on WRH's position (described in more detail below) that Access #1 was made by someone other than the WRH doctor, under the doctor's EMR user credentials, and that Access #2, while made by the WRH doctor, was made for the purpose of responding to a complaint filed against the doctor with the College of Physicians and Surgeons of Ontario.

[30] It is not strictly necessary for me to decide this issue in order to address Accesses #1 and #2 in the manner that I do, below. This is because my findings would be the same whether the WRH doctor were an agent of WRH or, alternatively, a health

---

[2] More particularly, "the person who operates" WRH is a health information custodian under this section of *PHIPA*.

[3] I acknowledge that in other situations, a physician with privileges at a hospital may be acting for his or her own purposes in handling personal health information, and thus act as an independent health information custodian under section 3(1). I address WRH's argument on this topic in the paragraphs that follow.

information custodian in his own right, in relation to the personal health information that was accessed.

[31] Nonetheless, in the interests of providing some guidance, I observe that both Accesses #1 and #2 occurred in the context of the WRH doctor's performance of his duties as a doctor with privileges at WRH. The accesses occurred because the doctor had logged into WRH's EMR in the course of performing those duties (Access #1), and, in the case of Access #2, because the doctor sought records to use in the College proceeding concerning the appropriateness of Access #1 (which access had occurred in the context of his hospital duties). There is no serious claim that the WRH doctor was acting independently of his hospital privileges in the circumstances of the accesses under review. As a result, in my view, in both situations the WRH doctor was an agent of WRH in respect of the personal health information at issue.[4]

Custody or control, and collection, use, and disclosure of personal health information in the shared EMR

Each of WRH and HDGH has custody or control of some patient personal health information in the shared EMR

[32] The accesses at issue in this complaint were made to records of the patient's personal health information contained in Solcom, the EMR shared by WRH and HDGH at the relevant times.

[33] The hospitals agree that they each have responsibilities under *PHIPA* (as well as under their data sharing agreement and each hospital's privacy policies) with respect to personal health information in the shared EMR. On this point, each hospital refers to and adopts the reasoning in PHIPA Decision 110, in which the IPC found that the various users of a shared EMR have responsibilities under *PHIPA* to protect the personal health information in that shared system.

[34] Both hospitals also agree that each hospital has custody or control of some of the personal health information in the shared EMR, and they take a consistent position on how to determine custody or control. Each considers a record of patient information created by a particular hospital (through its agents) to be a record in the custody or control of that hospital for the purposes of *PHIPA*. Using the terminology I applied above, in this complaint, this means, for example, that a discharge summary created by a WRH agent at WRH, and then uploaded to Solcom by WRH, is a "WRH record." Similarly, an outpatient clinic note prepared by an HDGH agent at HDGH, and uploaded to Solcom by HDGH, is an "HDGH record."

[35] I agree with the position taken by the hospitals, which is consistent with the IPC's approach to personal health information contained in shared systems.[5] When one

[4] Also see the discussion in PHIPA Decision 110 about the different scenarios in which a physician with privileges at a hospital may act as an agent of the hospital, or as an independent health information custodian.
[5] PHIPA Decisions 102 and 110.

hospital provides its records to the shared EMR, that hospital has certain obligations under *PHIPA* as the health information custodian with custody or control of the personal health information that it contributed to the shared system. When that record is then accessed by the other hospital (through the shared EMR), that other hospital also has certain obligations under *PHIPA* as a health information custodian with custody or control of the information it obtained through the shared EMR.

The accesses at issue involve collections, uses, and disclosures of personal health information in the shared EMR

[36] In the terminology of *PHIPA*, these transactions involve collections, uses, and disclosures of personal health information, as follows:

- A "collection" of personal health information occurs when one hospital (through its agents) obtains through the shared EMR a record contributed by the other hospital.[6]

- The same transaction involves a "disclosure" of personal health information by the hospital that contributed the record to the shared EMR.[7]

- When a hospital (through its agents) accesses a record of personal health information that the hospital itself created or contributed to the shared EMR, or a record that it has already collected from the shared EMR, that is a "use" of the personal health information in the record.[8]

[37] In this way, a transaction in which one hospital's agent accesses another hospital's record in Solcom has two components: a *collection* of personal health information by the first hospital (through its agent); and a corresponding *disclosure* of that same information by the second hospital to the first.

Any collection, use, or disclosure must comply with PHIPA

[38] It is important to note that in this transaction, both the collection and the disclosure must comply with *PHIPA*; so too must any subsequent use of that information. Section 29 of *PHIPA* requires that all collections, uses, and disclosures of

---

[6] Section 2 of *PHIPA* defines the term as follows: "'[C]ollect,' in relation to personal health information, means to gather, acquire, receive or obtain the information by any means from any source, and 'collection' has a corresponding meaning[.]"

[7] Section 2 of *PHIPA* defines the term as follows: "'[D]isclose,' in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information, and 'disclosure' has a corresponding meaning[.]"

[8] Section 2 of *PHIPA* defines the term as follows: "'[U]se,' in relation to personal health information in the custody or under the control of a health information custodian or a person, means to view, handle or otherwise deal with the information, subject to subsection 6 (1), but does not include to disclose the information, and 'use,' as a noun, has a corresponding meaning."
Section 6(1) clarifies that the providing of personal health information between a custodian and its agents is also a use (and not a disclosure) of that information.

personal health information be made with consent (from the individual to whom the information relates, or from another person authorized under *PHIPA* to give that consent), or otherwise be authorized (permitted or required to made) without consent by *PHIPA*.

[39] 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.

[40] WRH does not claim that the accesses at issue were made with consent from the appropriate person. Instead, WRH relies on various sections of *PHIPA* that permit a custodian to collect, use, and disclose personal health information, without consent, in certain circumstances. I will address the relevant sections of *PHIPA* under the appropriate headings, below.

[41] With this background in mind, I now consider WRH's responsibilities in respect of each of the accesses at issue in this complaint. (I address HDGH's responsibilities in respect of the common transactions in the related PHIPA Decision 177.)

ISSUES:

A. Should the complaint against the WRH doctor in respect of Accesses #1 and #2 proceed to a review?

B. Did WRH Employee A's use of the patient's personal health information comply with *PHIPA*?

C. Did WRH Employees A and B collect, and use, the patient's personal health information in compliance with *PHIPA*?

D. Did WRH's disclosure of the patient's personal health information to the HDGH doctor comply with *PHIPA*?

E. Did WRH take reasonable steps to protect personal health information in its custody or control? Did WRH respond appropriately to the complaint?

DISCUSSION:

A. Should the complaint against the WRH doctor in respect of Accesses #1 and #2 proceed to a review?

[42] During the complaint process, the parties advised the IPC that the complainant had also filed a complaint to the WRH doctor's regulatory body, the College of

Physicians and Surgeons of Ontario (the College), about the doctor's accesses to the patient's health records. The relevant College committee made a decision on the complaint, which at the complainant's request was later reviewed by the Health Professions Appeal and Review Board (the Board).

[43] This raises the question of whether the IPC should now exercise its discretion not to review the complaint against the WRH doctor about the same accesses.

[44] Section 57 of *PHIPA* sets out steps that may be taken by the IPC after receiving a complaint. Sections 57(3) and (4) address this office's authority to review or not to review a complaint. These sections state, in part:

> (3) If the Commissioner does not take an action described in clause (1) (b) or (c) [which relate to attempts at settlement] or if the Commissioner takes an action described in one of those clauses but no settlement is effected within the time period specified, the Commissioner may review the subject- matter of a complaint made under this Act if satisfied that there are reasonable grounds to do so.
>
> (4) The Commissioner may decide not to review the subject-matter of the complaint for whatever reason the Commissioner considers proper, including if satisfied that,
>
> > (a) the person about which the complaint is made has responded adequately to the complaint;
> >
> > (b) the complaint has been or could be more appropriately dealt with, initially or completely, by means of a procedure, other than a complaint under this Act[.]

[45] Section 57(4) sets out the IPC's authority not to review the subject-matter of a complaint for whatever reason it considers proper, including on certain specified grounds. One of these grounds, at section 57(4)(b), is the existence of another procedure that has dealt with, or could more appropriately deal with, the complaint before the IPC. The thrust of section 57(4)(b) is to confer a discretion on this office not to proceed with a complaint where doing so would amount to a re-litigation of issues addressed in another forum, or where a complaint to this office is premature.[9]

[46] In PHIPA Decision 80, the IPC considered whether to conduct a review of a complaint that had already been the subject of other proceedings. As in the complaint now before me, the prior proceedings considered in PHIPA Decision 80 were those of the College and the Board. In that case, the matter before the IPC was the same matter that had been considered by the College and the Board, involving allegations that a doctor had breached a patient's privacy.

---

[9] PHIPA Decision 80.

[47] In PHIPA Decision 80, the IPC concluded that it was appropriate to take notice of the existence of the prior proceedings, and of the issues considered in those proceedings, for the limited purpose of deciding whether they had appropriately dealt with the matter brought to the IPC, and thus whether the IPC should exercise its discretion under *PHIPA* not to review the matter.[10]

[48] In that decision, the IPC set out some factors for consideration in its exercise of discretion under section 57(4)(b). These factors include: the issues in the other procedure, and how they relate to the issues before the IPC; the purpose and scope of the other procedure; the jurisdiction of the body conducting the other procedure; whether the other procedure was procedurally fair to the parties; and whether it would be unfair or unjust not to proceed with a review in the circumstances. These questions assist in determining whether the substance of a complaint has been "appropriately dealt with," and whether, in any case, fairness to the parties militates in favour of reviewing the matter.[11]

[49] During the review stage, the IPC asked the parties to comment on whether, in light of all relevant factors, the complaint against the WRH doctor in respect of these accesses ought to proceed to a review under *PHIPA*.

The parties' representations

[50] WRH asks the IPC to exercise its discretion under section 57(4)(b) not to review this matter. This is based on the fact (which is not disputed by the complainant) that the complainant complained to the College about these same actions and conduct by the WRH doctor, and obtained a decision from the College (through its Inquiries, Complaints and Reports Committee). At the complainant's request, the College committee's decision was later reviewed by the Board.

[51] WRH submits that relevant factors support a finding that these other proceedings "appropriately dealt with" the issue now before me, and were procedurally fair, so that the IPC should exercise its discretion under section 57(4)(b) not to review the matter. WRH's submissions on this topic are detailed, and the complainant does not challenge their accuracy. In summary, WRH submits that: the College and Board had jurisdiction to address the complaint about the doctor's actions; the substance of the complaint to the College (and reviewed by the Board) is the same as the substance of the complaint now before me; the College and Board processes were procedurally fair to all parties; and the College (through the committee) made a determination on the complaint, following which the complainant exercised his right to request a review of the decision by the Board.

[52] WRH also submits that it would not be unfair or unjust for the IPC not to review

---

[10] PHIPA Decision 80, para 78. The IPC concluded that section 36(3) of the *Regulated Health Professions Act, 1991* (SO 1991, c 18) does not preclude the IPC from taking notice of the prior proceedings for the limited purpose of making a determination under section 57(4)(b) of *PHIPA*.

[11] PHIPA Decision 80, referring to *British Columbia (Workers' Compensation Board) v. Figliola*, 2011 SCC 52 (CanLII), and *Penner v. Niagara (Regional Police Services Board)*, 2013 SCC 19 (CanLII).

this issue, which has already been addressed through these other proceedings, while there would be prejudice to the hospital and the WRH doctor if the matter were to be addressed again by the IPC. Among other reasons, WRH notes that the parties have already dedicated time and resources to address this complaint through the prior proceedings, and that all parties have an interest in the finality of these matters.

[53] For his part, the complainant does not dispute that his complaint about the WRH doctor was considered by the College, and then by the Board, at his request. He does not claim that the substance of the complaint he made to those bodies is different from the substance of his complaint to the IPC about the WRH doctor. He does not specifically refer to any of the factors identified above. Instead, the complainant focuses primarily on a different concern, which is his dissatisfaction with the information WRH provided to him about the circumstances of Access #1. This relates to WRH's changing explanation for this access, as I describe below.

[54] During the earlier stages of the complaint, WRH took the position that the WRH doctor's Access #1 was made for the purposes of a quality review (and was on this basis an authorized use under *PHIPA*). However, in its representations during the adjudication stage, WRH stated that it has since received new information, and now believes the access was made by another WRH agent, and by not the WRH doctor.

[55] This new information appears to have raised by the WRH doctor during the course of the College proceedings. Based on this information, WRH now believes that on the date of Access #1, the doctor failed to log out of his Solcom account after using one of two shared (common) EMR terminals in WRH's emergency department, and that another WRH agent (and not the doctor) accessed the patient's records, under the doctor's EMR user credentials.

[56] As I discuss in more detail below under Issue E (addressing the adequacy of WRH's response to this complaint), WRH reports that it is conducting an investigation to determine which of its agents was responsible for Access #1. It acknowledges that given the passage of time, it may never be able to determine with certainty which agent made this access, and for what purpose. Nonetheless, WRH confirms that the doctor's failure to log out of the shared EMR was a breach of its privacy policy, and it described other steps it has taken to address this contravention of its privacy policy (and of *PHIPA*) that led to Access #1.

[57] The complainant argues that WRH ought to have given him this new explanation for Access #1 much earlier than it did. Instead, he says, the new explanation emerged during the course of the other proceedings, and not when he initially filed his complaint with the College (or with the IPC) about this access. He asks why WRH has not investigated the matter. The complainant also submits that WRH's revelation that some other WRH agent was responsible for Access #1 is a fresh privacy breach for which he ought to have received notice under *PHIPA*.

[58] The WRH doctor (whom I notified as an affected party in this complaint) supports WRH's request that I decline to conduct a review of Access #1. In addition, he

advises that the complainant's concerns about his Access #2 were also considered by the College and the Board in the prior proceedings, and he submits that I should decline to conduct a review of both accesses on the same basis. In support of his statement, he refers to the Board's decision on this matter, which is a public decision.

[59] In response to the WRH doctor's representations, the complainant largely repeats the concerns I have summarized above. He also raises a concern that Access #2 (which the WRH doctor does not deny having made) involved more personal health information than was needed for the claimed purpose of this access. This is an argument that I will address briefly in my analysis, below. He also submits that neither the Board nor the College has expertise in privacy law, while the IPC has such expertise, and that these bodies failed to properly investigate what happened and to make an appropriate decision.

[60] In general, it is clear from the complainant's representations that he is dissatisfied with the decisions of the College and the Board in response to his complaint about the WRH doctor's accesses, and is seeking a different result from the IPC.

Analysis and findings

[61] For the reasons that follow, I decline to conduct a review of the complaint against the WRH doctor in relation to Accesses #1 and #2. However, I will address as a separate matter (at Issue E, below) some broader concerns raised by the complainant about the hospital's handling of the complaint, which were not addressed by the prior proceedings.

[62] On the question of whether to conduct a review of the complaint against the WRH doctor in respect of these accesses, I have considered the prior proceedings cited by the parties only to the extent necessary for making a determination under section 57(4)(b) of *PHIPA*. Specifically, I have looked at the public decision of the Board to verify the doctor's statement that the issues before me were raised in the proceedings before the College and the Board. It is clear from the Board's public decision that the complainant raised the matter of Accesses #1 and #2 in his complaint to the College about the WRH doctor, and that the substance of the complaint to the College (and later considered by the Board) is identical to the complaint brought to the IPC about the doctor.

[63] In deciding not to conduct a review of the complaint against the WRH doctor about these accesses, I have considered the relevant factors summarized above.

[64] First, I accept that the College had jurisdiction to address the matter. While the complainant submits that the IPC has special expertise in privacy law, there is no question that the College also has the authority to receive complaints about privacy breaches by its members. As noted by the parties, the IPC has recognized this function of the College in prior decisions, including in PHIPA Decisions 35 and 80. In these decisions, the IPC recognized that the College's mandate to respond to public complaints about its members' conduct and actions may include investigating

complaints about a member's failure to maintain the confidentiality of patient information in accordance with professional and legal obligations.

[65] There is no dispute that at the complainant's request, the Board reviewed the College committee's decision, as the Board is authorized to do under the *Regulated Health Professions Act, 1991*.

[66] There is no claim that the College and Board proceedings were procedurally unfair. There is also no claim that the substance of the matter before those bodies is different from the one now before me.

[67] Based on these relevant factors, I conclude that the proceedings before the College and the Board "appropriately dealt with" the complaint against the WRH doctor in respect of Accesses #1 and #2.

[68] I find, furthermore, that there is no unfairness to the parties in declining to review this matter under *PHIPA*.

[69] I agree with and follow the finding in PHIPA Decision 80 in recognizing there are differences in the purpose and scope of proceedings before the College and the Board, and those before the IPC, in light of the bodies' different mandates. In addition, the available outcomes are different, and serve different purposes.[12] In particular, dispositions issued by the College (through its various committees) are generally directed at improving an individual member's conduct or future practice, or disciplining the member where appropriate, while the IPC's focus is on addressing systemic issues arising from complaints.[13]

[70] In this case, these differences present no reason for me to re-examine the complaint against the WRH doctor. The complainant's submissions indicate that in asking the IPC to revisit this issue, his purpose is to obtain a more severe outcome for the WRH doctor. In this way, what the complainant seeks is more akin to another assessment of the College committee's decision, because he is dissatisfied with the Board's assessment, and he believes a different result is appropriate. But this is not the function of the IPC.

[71] I considered similar arguments by the requesting party in PHIPA Decision 80, and in that case too I declined to conduct a review where the party was seeking more severe remedies that the College could have imposed (but did not impose) on its member. As in that decision, I observe here that fairness considerations are not engaged simply because a party believes that the prior proceedings should have yielded different results. The IPC has affirmed, in a different context, that its statutory role is not to evaluate the severity or appropriateness of particular sanctions imposed against a party for a violation of *PHIPA*.[14]

---

[12] PHIPA Decision 16, at para 19, and PHIPA Decision 80 at para 86.
[13] PHIPA Decision 80, at para 86.
[14] PHIPA Decision 80, at paragraph 88, citing Orders HO-002 and HO-010, and PHIPA Decision 74.

[72] Having found that the College and Board proceedings addressed the same issue regarding the WRH doctor, that they were authorized to do so, and that they satisfied the other criteria described above, I conclude that fairness militates in favour of finality in this case, and I decline to conduct a review of the complaint against the doctor in respect of these accesses.

[73] However, I will consider later in this decision relevant aspects of WRH's handling of the complaint about the doctor's actions. The IPC's review of this broader matter is appropriate, given the IPC's focus on systemic issues such as the adequacy of a custodian's training of its agents, and the appropriateness of its response to privacy breaches. (I also confirm that these issues were not addressed in the prior proceedings, which concerned the conduct of the member doctor.) I will also consider the complainant's allegations that WRH has not investigated the circumstances behind Access #1, and that WRH had a duty to notify him of a new privacy breach.

[74] Before I leave this topic, I wish to briefly address the complainant's allegation that the WRH doctor's Access #2 involved more personal health information than was strictly needed for the stated purpose of this access. Specifically, the complainant states that it should not have been necessary for the WRH doctor to access on this occasion a particular clinical note. As stated above, using (or collecting, or disclosing) more personal health information than is reasonably necessary to meet the purpose of the use (or collection or disclosure) is contrary to the limitation principle in section 30 of *PHIPA*.

[75] I have found that the WRH doctor's Accesses #1 and #2 were raised at the prior proceedings, and I thus decline to review them here. However, for the benefit of the complainant, I make the following observations. First, I note that the records that are alleged to have been accessed on the occasion of Access #2 are identical to those that were the subject of Access #1. I further note that it is the doctor's (and WRH's) position that the doctor's Access #2 was made for the purpose of addressing the College complaint against him regarding Access #1.[15] While I make no finding on the appropriateness of Access #2, I note generally that in the case of an authorized use for the purpose of a proceeding, it would not be unreasonable to expect relevant records to include all the records that are at issue in the proceeding.

[76] For all the reasons given above, applying the relevant considerations of judicial finality, economy, and fairness, I exercise my discretion under section 57(4)(b) to decline to conduct a review of the complaint against the WRH doctor in relation to Accesses #1 and #2.

---

[15] WRH refers to section 37(1)(h) of *PHIPA*, which permits a custodian to use personal health information without consent "for the purpose of a proceeding or contemplated proceeding in which the custodian or the agent or former agent of the custodian is, or is expected to be, a party or witness, if the information relates to or is a matter in issue in the proceeding or contemplated proceeding." Section 37(2) permits a custodian to provide personal health information to its agent for the same authorized use.

B. Did WRH Employee A's use of the patient's personal health information comply with *PHIPA*?

[77] This aspect of the complaint concerns the access by WRH Employee A to various WRH records in Solcom (an emergency record, discharge summary, consultation note, and mental health form). This access occurred six days after the patient's death.

[78] As explained above, this access is a "use" of the patient's personal health information by WRH Employee A, because the WRH agent accessed various Solcom records that originated from WRH. The question under this heading is whether the agent's use of the patient's personal health information complied with *PHIPA*. For the reasons that follow, I find it was an authorized use under section 37(1)(d) of *PHIPA*.

[79] Section 37(1)(d) permits a custodian to use personal health information, without consent, "for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian." An agent's use of personal health information, on behalf of the custodian, for this same purpose is authorized by section 37(2) of *PHIPA*.

[80] WRH explains that at the time of this access, WRH Employee A was WRH's Regional Vice-President, responsible for portfolios including patient relations and legal affairs. In this role, WRH Employee A was responsible for managing relationships between patients and the hospital, and performing quality assurance duties, including reviews under the *Quality of Care Information Protection Act, 2016* (*QCIPA*).[16] WRH explains that at the time of this access (six days after the patient's death), WRH Employee A would have anticipated a *QCIPA* review into the circumstances of the patient's death, and the need for WRH staff to meet with the patient's family. In fact, WRH Employee A ultimately led the *QCIPA* review of the circumstances around the patient's death.

[81] In his responding representations, the complainant questions why WRH did not invite HDGH to participate in its *QCIPA* review. He has other criticisms about WRH's processes, which I will briefly address further below. However, I do not find these broader comments to be relevant in deciding the issue of whether this particular access complied with *PHIPA*.

[82] Given the circumstances of the patient's death, and WRH Employee A's role at the hospital to manage patient relations and legal matters, I find it was reasonable for the employee to anticipate the need for a hospital investigation and meetings with the family to address issues around the quality of care provided to the patient. I find these are risk and error management activities, and activities to maintain and improve the quality of care and related hospital programs and services, within the meaning of

[16] SO 2016, c 6, Sch 2. The purpose of *QCIPA* is to enable confidential discussions and information-sharing about errors, systemic problems and quality improvement opportunities in the health care system (section 1 of *QCIPA*).

section 37(1)(d).

[83] In addition, there is no evidence to suggest that WRH Employee A's use of personal health information for this authorized purpose contravened the limitation principle in section 30.

[84] I conclude this access was an authorized use without consent under *PHIPA*.

C. Did WRH Employees A and B collect, and use, the patient's personal health information in compliance with *PHIPA*?

[85] At issue under this heading are the accesses by WRH Employees A and B to certain HDGH patient records in Solcom.

[86] The access by WRH Employee A occurred six days after the patient's death, and involved the following HDGH records: a clinic record, a clinic note, and a crisis note.

[87] The access by WRH Employee B occurred several months after the patient's death. For reasons I explain further below, WRH is unable to ascertain exactly which records WRH Employee B accessed on this occasion.

[88] As explained above, these transactions involve "collections" of personal health information by WRH Employees A and B, because the records they accessed in Solcom originated from HDGH. (The related PHIPA Decision 177 addresses the role of HDGH in relation to the aspects of these same transactions that constitute "disclosures" by HDGH of this information to the WRH agents.) I must also consider the WRH agents' subsequent "use" of this personal health information. Therefore, the issue under this heading is whether these collections, and uses, of personal health information by WRH agents complied with *PHIPA*. For the reasons that follow, I find they complied with *PHIPA*.

[89] As explained above, WRH Employee A was at the relevant time WRH's Regional Vice-President, responsible for portfolios including patient relations and legal affairs.

[90] At the relevant time, WRH Employee B also had patient relations responsibilities, in her role as a hospital Patient Representative. WRH explains that patient representatives assist patients and their family members with issues related to the delivery of hospital services, and this can include conflict resolution duties. WRH states that in this role, WRH Employee B met with the patient's family on two occasions. WRH Employee B also co-led (with WRH Employee A) the *QCIPA* review that was conducted into the circumstances of the patient's death.

[91] As noted above, WRH Employee A's access to HDGH records occurred six days after the patient's death.

[92] WRH Employee B's access occurred about nine months after the patient's death. WRH places the timing of WRH Employee B's access in context by explaining that it occurred in between her first and second meetings with the family. WRH Employee B's

first meeting with the family occurred after the completion of the *QCIPA* review (which occurred about six months after the patient's death). After this first meeting, WRH Employee B accessed HDGH records in preparation for her second meeting with the family. This second meeting was held to discuss the care that had been provided to the patient, the hospital's commitment to quality improvement measures, and the family's formal complaint to the hospital. The second meeting ultimately took place four months after WRH Employee B's access to the HDGH records.

[93] The complainant was invited to respond to WRH's explanations for these accesses. As noted above, the complainant made comments that relate broadly to WRH's *QCIPA* review, and other hospital processes. They do not bear directly on the issue of whether the accesses at issue complied with *PHIPA*.

[94] Based on the evidence, I am satisfied that WRH Employees A and B accessed the HDGH records in Solcom for purposes related to risk and error management, and to maintain and improve the quality of hospital programs and services. On this basis, I find that *PHIPA* authorized these collections and uses to be made without consent.

[95] Specifically, I accept WRH's submission that the collections at issue were authorized to be made under section 36(1)(c)(iii) of *PHIPA*. This section states:

> A health information custodian may collect personal health information about an individual indirectly if the custodian is an institution within the meaning of the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act*, or is acting as part of such an institution, and the custodian is collecting the information for a purpose related to the statutory function of the custodian[.]

[96] As a hospital, WRH is an institution within the meaning of the *Freedom of Information and Protection of Privacy Act* (paragraph (a.2) of the definition of "institution" in that statute). WRH submits, and I accept, that its agents' collection of personal health information was made for quality of care and risk management purposes that directly relate to the hospital's statutory functions, including under the *Public Hospitals Act* and *QCIPA*, to provide quality health care.

[97] These collections were also authorized under section 36(1)(g) of *PHIPA*. This section permits a custodian (or, in this case, agents of the custodian) to collect personal information health from a person who is "permitted or required by law […] to disclose it to the custodian." In PHIPA Decision 177, I find that in these same transactions, HDGH was authorized to disclose this personal health information to the WRH agents under section 39(1)(d) of *PHIPA* (disclosure to another custodian to improve or maintain quality of care). As a result, the corresponding collections of this same information by the WRH agents complied with section 36(1)(g).

[98] Turning now to the subsequent use of the personal health information by WRH Employees A and B, I find these actions also complied with *PHIPA*.

[99] The agents' use of this information was authorized under section 37(1)(a) of *PHIPA*, which permits the use of personal health information for the purposes for which the information was collected. Having collected the records for quality of care and risk management purposes, and in the absence of any evidence to the contrary, I accept that the WRH agents then used the records for these same purposes.

[100] Their use of personal health information was also authorized under section 37(1)(d), which permits the use of personal health information for risk management, error management, or activities to improve or maintain the quality of care or related hospital programs or services.[17] For the same reasons given above under the previous heading, I am satisfied that WRH Employees A and B used the personal health information at issue to investigate the circumstances of the patient's death and to respond to the patient's family, which are risk and error management activities and activities to maintain and improve the quality of care and hospital programs and services, within the meaning of section 37(1)(d).

[101] Lastly on this topic, as noted above, the collection and use of personal health information must comply with section 30 of *PHIPA*. This means, among other things, that no more personal health information should be collected and used than is reasonably necessary to meet the purpose of the collection and use.

[102] As described above, WRH Employee A's collection and use involved the following HDGH records: a clinic record; a clinic note; and a crisis note. I have no evidence before me to suggest that this collection and use contravened the data minimization principles in section 30.

[103] With respect to WRH Employee B, WRH states that it is unable to identify precisely which HDGH records were collected and used by WRH Employee B on the date in question. This is because at the request of the complainant, the patient's electronic health record has been locked, preventing WRH (and HDGH) from identifying the particular HDGH records that were accessed on that date. However, WRH's audit indicates that the access lasted less than two minutes.

[104] The complainant made no comment on WRH's statements on this issue. There is no claim by the complainant nor any evidence before me to suggest that WRH Employee B's collection and use of personal health information involved more personal health information than was reasonably necessary for the purposes outlined above, or otherwise contravened section 30. In the circumstances, I see no reason to believe the collection and use did not comply with *PHIPA*.

[105] More generally, to address the complainant's objection to WRH agents' having accessed HDGH records in this context, I find reasonable, and persuasive, WRH's explanation that examining records of the care the patient received at HDGH was a relevant part of WRH's assessment of the overall quality of care provided to him.

---

[17] As noted above, section 37(2) permits a custodian's agents to use personal health information for the purposes authorized in section 37(1) of *PHIPA*.

[106] I conclude that WRH Employees A and B collected and used personal health information in compliance with *PHIPA*.

D. Did WRH's disclosure of the patient's personal health information to the HDGH doctor comply with *PHIPA*?

[107] Under this heading, I will consider, in relation to WRH's obligations, the HDGH doctor's access to a WRH record (a discharge summary authored by a physician at WRH) in Solcom. This access occurred seven days after the patient's death, and lasted approximately one minute.

[108] As explained above, this access by the HDGH doctor involves a "disclosure" by WRH to an agent of HDGH. (I address the corresponding "collection" of this same information by the HDGH doctor in PHIPA Decision 177.) The question under this heading is whether WRH's disclosure of personal health information complied with *PHIPA*.

[109] For the reasons that follow, I conclude that the disclosure was authorized under section 39(1)(d) of *PHIPA*. This section states:

> Subject to the requirements and restrictions, if any, that are prescribed, a health information custodian may disclose personal health information about an individual […] where,
>
> > (i) the disclosure is to another custodian described in paragraph 1, 2 or 4 of the definition of "health information custodian" in subsection 3 (1),
> >
> > (ii) the individual to whom the information relates is one to whom both the disclosing custodian and recipient custodian provide health care or assist in the provision of health care or have previously provided health care or assisted in the provision of health care, and
> >
> > (iii) the disclosure is for the purpose of activities to improve or maintain the quality of care provided by the receiving custodian to the individual to whom the information relates or individuals provided with similar health care.

[110] I am satisfied that all three conditions in section 39(1)(d) were met in this case. I note here that no prescribed requirements or restrictions apply to the disclosure considered under this heading.

[111] First, the disclosure was made to an agent of HDGH, which is a health information custodian within the meaning of paragraph 4 of section 3(1) of *PHIPA*. This fulfils the condition in paragraph (i) of section 39(1)(d).

[112] Second, the personal health information at issue relates to a patient to whom both WRH and HDGH provided health care, fulfilling the condition in paragraph (ii).

[113] The third condition in section 39(1)(d) is that the disclosure be for the purpose of activities to improve or maintain the quality of care provided by the receiving custodian (here, HDGH), either to the patient, or to other individuals to whom HDGH provides similar health care.

[114] WRH and HDGH explain that before the patient's death, the HDGH doctor provided care to the patient at HDGH's General Psychiatry Clinic (the clinic) within its Transitional Stability Centre, a crisis wellness centre. In addition to this care role, the HDGH doctor has a leadership role at the clinic, in which he is responsible for overseeing the quality of care at the clinic, and for creating, revising, and overseeing the clinic's policies and procedures. The hospitals submit that in this context, WRH appropriately disclosed to the HDGH doctor (and the HDGH doctor appropriately collected) the patient's personal health information for the purpose of improving and maintaining the quality of mental health care provided by HDGH to patients of its clinic.

[115] The complainant challenges the HDGH doctor's need to access the particular record he did (a discharge summary prepared by a WRH physician), given that the HDGH doctor had stopped treating the patient some time before the patient's death.

[116] It is clear that the disclosure in this case was made after the patient's death, and there is no claim the disclosure was relevant to the quality of care provided to the patient. However, section 39(1)(d) clearly contemplates the disclosure of personal health information for purposes relating to the care given to other patients (meaning patients other than the individual to whom the personal health information relates).

[117] Considering the circumstances of the patient's death and the HDGH doctor's roles as both care provider and administrator of the clinic, I am satisfied that WRH's disclosure to HDGH met the requirements of section 39(1)(d). This is because I accept that the purpose of the disclosure by WRH was to improve or maintain the quality of mental health care provided by HDGH to its patients. (For related reasons, I find in PHIPA Decision 177 that HDGH's corresponding collection of this same information also complied with *PHIPA*.)

[118] I am also satisfied that this disclosure, consisting of a discharge summary prepared by a WRH physician, complied with the data minimization principle in section 30 of *PHIPA*. In particular, I see no basis to conclude that WRH disclosed (and that the HDGH doctor collected) more personal health information than was reasonably necessary for the quality of care purposes of the access.

[119] I conclude that WRH's disclosure of personal health information complied with *PHIPA*.

E. Did WRH take reasonable steps to protect personal health information in its custody or control? Did WRH respond appropriately to the complaint?

[120] *PHIPA* requires health information custodians to take reasonable steps to protect personal health information in their custody or control, including against unauthorized

collection, use or disclosure. Section 12(1) of *PHIPA* 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.

[121] 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.[18]

[122] A related obligation is the duty for health information custodians to have in place and to comply with information practices, including administrative, technical and physical safeguards and practices with respect to personal health information in their custody or control [sections 2, 10(1) and 10(2)].

[123] 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, and the consequences of failing to comply with these obligations.[19] Custodians remain responsible for any personal health information handled on their behalf by their agents.[20]

[124] In this context, I will consider some of the additional concerns raised by the complainant about WRH's handling of his complaint about unauthorized accesses, and about WRH's privacy and other practices.

The hospital took reasonable steps to protect personal health information in the EMR, and responded adequately to the complaint

[125] Under this heading, I will consider the hospital's responsibilities in relation to the WRH doctor's Access #1, and the adequacy of the hospital's response to the complaint about this access. These broader issues were not before the College or the Board, which dealt with the complaint against the WRH doctor himself in relation to his accesses. I will also consider the broader issue of whether the hospital had in place reasonable measures to protect the security of personal health information in the shared EMR.

[126] As noted above, the WRH doctor has now explained that Access #1 was not made by him, though made under his EMR user credentials. The doctor believes he neglected to sign out of his Solcom account after using the common EMR terminal in WRH's emergency room, and that another WRH agent used the same terminal to access the patient's records. Prior to having this new information, WRH had taken the

---

[18] PHIPA Decision 44, at para 140. See also PHIPA Decisions 74, 80, 110, and 168, among others.
[19] See, for example, sections 12(1), 15(3)(b), and 17.
[20] Section 17(3)(b).

position (at earlier stages of the IPC process) that the WRH doctor's Access #1 was justified on other grounds in *PHIPA*.

[127] During the review, the complainant took issue with the fact he only became aware of this new explanation for Access #1 during the course of the College proceeding. He also complained that he had not received notification of this privacy breach from WRH (referring to the obligation in section 12(2) of *PHIPA* that custodians notify affected individuals of a privacy breach at the first reasonable opportunity). He also questioned why WRH is not investigating the matter.

[128] At the date of its representations to the IPC, WRH stated that it was in the process of investigating which of its agents made this access. This addresses the complainant's request that WRH investigate. I note that the complainant asks to be informed of the results of WRH's investigation, and I trust that WRH will do so.

[129] Although the complainant is dissatisfied that the new explanation for Access #1 emerged only during the College proceeding, and not when he initially filed his complaint with WRH, the information before me does not suggest any intention to mislead on WRH's part. The WRH doctor's new explanation appears to have emerged after he had an opportunity to see the records he was alleged to have accessed on the date of Access #1. I see no fault in WRH's having accepted the doctor's initial explanation for the access, or any undue delay in its manner of communicating the new explanation to the IPC and the complainant (who was already aware of the new explanation from his participation in the College proceeding).

[130] I also see no basis for requiring additional notice to the complainant in these circumstances. The complainant was already aware (through the audit results) of Access #1, and had questioned its appropriateness. The matter of Access #1 was already the subject of a complaint to the College, and a complaint to the IPC. In these circumstances, the WRH doctor's changing explanation for this access did not give rise to a different privacy breach requiring fresh notification. I note that one of the purposes of the breach notification provisions in *PHIPA* is to permit the affected individual to make a complaint to the IPC [section 12(2)(b)]. In this case, the complainant had already filed complaints about this same access. There would be no purpose served by requiring WRH to provide a fresh notice to the complainant under section 12(2).

[131] Next, I will consider the broader question of whether the hospital had in place reasonable measures to protect the patient's personal health information in the shared EMR, and the steps the hospital has taken to respond to the complaint.

[132] In this complaint, WRH acknowledges that the WRH doctor acted in contravention of its policies in respect of Access #1. Specifically, WRH provided a copy of its privacy policy to show that the doctor's failure to log out of the shared Solcom terminal was a breach of hospital procedure. To address this breach, the hospital issued a written caution to the doctor, which will be retained in the doctor's Medical Affairs file. In deciding on this disciplinary action, WRH also considered the outcome of the College and Board proceedings against the doctor. WRH says that it is satisfied the WRH doctor

now understands that he failed to comply with his duties under the hospital's policies and procedures, and under *PHIPA*, to maintain the security of patient information.

[133] WRH also recognizes its own responsibility, as the custodian, to have in place and to adequately train its agents on its policies and procedures to protect personal health information. At the IPC's request, the hospital described the administrative, technical, and physical safeguards in place to protect the security of patient information in the shared EMR, both at the time of the accesses at issue and currently.

[134] WRH provided a copy of its data sharing agreement with HDGH in respect of the shared EMR. Staff at both hospitals with access to the shared system are also required to sign the confidentiality agreements of each hospital. All WRH staff are required to sign the WRH confidentiality agreement upon hire, and to re-sign annually. WRH also provided details of the initial and annual privacy training, and attestation regarding the training, that it requires all hospital EMR users to complete.

[135] WRH advised that professional staff (such as doctors) are required to document in the shared EMR any accesses made for quality assurance purposes. After learning that the WRH doctor had been unaware of this obligation, WRH legal and privacy staff provided refresher training to professional staff on why and how to document in the shared EMR any accesses made for quality assurance purposes. Further, in response to this incident, WRH circulated a memorandum to all staff to remind them of their obligations under the hospital's policies and *PHIPA* to protect patient information, and of the hospital's measures to prevent and to detect unauthorized access. This included a reminder about the auditing features available through the hospital's new EMR system, Cerner (which I will discuss in more detail further below).

[136] WRH also explained that regular audits are one of the technical safeguards in place to protect patient information in the EMR. Others include the use of unique staff passwords and user IDs, and strong encryption, firewalls and virus scanning provided by its shared service provider. WRH also provided a copy of the privacy notice flag that appears before users can enter the EMR system. Among other things, this notice: warns users against accessing personal health information except for authorized purposes such as the provision of health care; informs users that their accesses in the EMR are monitored by the hospital; and describes disciplinary actions that can be taken in the case of unauthorized access, including termination of employment, reporting to the user's regulatory college and to the IPC, legal action, fines, and penalties.

[137] Finally, WRH described physical safeguards, including paper notices at point-of-use sites warning against unauthorized use of patient personal health information, and the strategic placement of computer workstations in areas frequented only by authorized staff.

[138] In April 2021, for reasons unrelated to this complaint, WRH adopted a new shared EMR system, called Cerner. WRH explains that the above practices continue to apply to users of the new EMR. In addition, before its implementation, the hospital provided training to all EMR users on the new system, and refresher training on areas

such as the need to properly document quality assurance activities in the EMR. Staff were required to complete this training before being granted access to the new system.

[139] WRH also describes some features of the new Cerner system that improve the hospital's ability to maintain the security of patient personal health information. Most relevant in the context of this complaint are the following features of the new system:

- A "tap and go" log-in and log-out system that enables users to log on and off by tapping a card or fob to the screen;
- Automatic log-out after five minutes of user inactivity; and
- A robust auditing feature that, according to the software provider, enables routine and detailed security auditing (including by identifying areas of risk and anomalies in behaviour patterns) and provides customized alerts.[21]

[140] WRH also explains that the new Cerner system will eventually enable shared access to patient records by all health service providers within the Windsor-Essex Ontario Health Team,[22] with the expectation that all providers will participate on a regional privacy committee and adopt a uniform privacy breach protocol. Shared systems of this nature can provide many benefits to participating custodians, so long as they are subject to a strong governance framework, including harmonized privacy policies and procedures. In this regard, I refer WRH, HDGH, and the other participating custodians to IPC guidance on this topic, including particularly PHIPA Decision 102.[23]

[141] Overall, taking into account the measures WRH had in place at the time of the accesses at issue, and the measures implemented since that time (including, most notably, the improved security features of its new EMR), I am generally satisfied that WRH complied with its obligations under section 12(1) to take reasonable steps to protect personal health information in its custody or control.

[142] Considering that Access #1 occurred because the WRH doctor neglected to log out of the shared EMR, I agree that features of the new system (particularly the more convenient method of logging in and out, and the timed automatic log-out) will help to reduce the risk of future unauthorized accesses in the nature of Access #1. I also find helpful in this regard the actions taken by WRH to identify and to address gaps in the training of its agents that were revealed through Access #1. This includes WRH's reminders to its agents about documentation requirements in the EMR and about the hospital's auditing practices. These measures reinforce privacy-protective behaviours among hospital staff, which helps to reduce the risk of unauthorized access.

[143] I am also satisfied that WRH has complied with the related duty in section 12(1)

---

[21] https://www.cerner.com/solutions/p2sentinel.
[22] https://www.weoht.ca/aboutOHTs.
[23] Also PHIPA Decisions 62 and 110; and Information and Privacy Commissioner of Ontario, *Detecting and Deterring Unauthorized Access to Personal Health Information* (January 2015). Available online: https://www.ipc.on.ca/wp-content/uploads/Resources/Detect_Deter.pdf.

to respond adequately to this complaint. After learning of the complaint to the IPC, the hospital investigated each of the accesses identified by the complainant, including by consulting with HDGH as necessary. Through this process, and the sharing of information at earlier stages of the complaint, the parties were able to resolve the complainant's concerns about some of the accesses, and to remove these from the scope of the complaint.

[144] At a later stage of the complaint process, after receiving new information about the circumstances of Access #1, the hospital provided this information to the IPC along with an account of the steps it had taken to address the matter. As noted above, WRH continues to investigate Access #1, although it has acknowledged that given the passage of time, it may not be possible to determine with certainty which agent made this access, and for what purpose. Whatever the outcome, I expect WRH to inform the complainant. I also take into account the full cooperation shown by WRH (as well as by the complainant) in this complaint process.

[145] For all these reasons, I am generally satisfied that WRH has complied with its duties under section 12(1) of *PHIPA*. However, I want to make some comments to assist WRH in meeting its obligations under *PHIPA* in future.

[146] The first has to do with the circumstances of Access #1. WRH has acknowledged that in failing to log out of his Solcom account, the WRH doctor contravened the hospital's policy, and it has taken steps (including disciplinary measures) to address the doctor's conduct. However, in another part of its representations, WRH is equivocal about the actions of the unknown WRH agent who accessed the patient's records under the doctor's EMR credentials. Specifically, WRH says it is possible this agent accessed the patient's health records for an authorized purpose under *PHIPA*.

[147] I want to clarify for WRH's benefit that whatever the agent's purpose in accessing the patient's records on that date, the access made under another user's EMR credentials, in contravention of the hospital's policy, is itself a contravention of *PHIPA*.[24] This is the case even if WRH later determines through its investigation that the access was made for some purpose that would otherwise be authorized under *PHIPA* (such as a quality assurance purpose).

[148] I considered a similar claim by a custodian in PHIPA Decision 110. In that case, the custodian proposed that the sharing of EMR user credentials between its agents, when done to enable the collection and disclosure of patient information for health care purposes, complied with *PHIPA*. However, as in the case now before me, the sharing of EMR user credentials contravened the custodian's own information practices, which as noted above is itself a contravention of *PHIPA*. The practice of sharing EMR user credentials should also be discouraged because it could allow unauthorized users to have undetected access to a custodian's EMR.

[149] The custodian in PHIPA Decision 110 later amended its information practices to

[24] Sections 10(2) and 17(4)(a). See also PHIPA Decisions 110 and 168.

make clear to its agents that they must not share their EMR user credentials in any circumstances. I recommend that WRH do the same, through amendments to its privacy policy, EMR user agreements, and other relevant information practices.

[150] Finally, I want to acknowledge the complainant's comments, made throughout his representations, about his dissatisfaction with specific hospital processes. These are largely focused on what he identifies as deficiencies in WRH's *QCIPA* review process. They include his concerns that WRH did not include HDGH in its *QCIPA* review concerning the patient, even though hospital agents considered HDGH records in the course of this review, and the hospital's admission that it has no formal policy outlining the steps in a *QCIPA* review (because, the hospital says, the process is not complex).

[151] I have already addressed, above, the specific instances in which WRH agents accessed HDGH records for the purpose of the *QCIPA* review and for other quality of care purposes. I also noted above the steps WRH has taken to address some deficiencies in its training of professional staff on documentation requirements when they access personal health information for quality assurance purposes. These are matters properly addressed under *PHIPA*.

[152] However, the complainant's broader concerns about the hospital's *QCIPA* process are outside the scope of this review, and are better addressed directly to the hospital. I recognize that the hospital has already attempted to respond to some of these concerns in its representations filed during this review process. I hope that by directly communicating on some of these issues, the parties are able to address the complainant's wish for a better understanding of the *QCIPA* process that occurred here.

[153] For all the reasons given above, and taking into consideration the guidance provided by this decision, I conclude that WRH complied its obligations under *PHIPA*. I dismiss the complaint.

NO ORDER:

For the foregoing reasons, I conclude my review without issuing any order.

However, I recommend that WRH amend its information practices to clearly prohibit the sharing of EMR user credentials between its agents.

Original Signed by: April 5, 2022

Jenny Ryu
Adjudicator