Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 177

Complaint HC19-00055

Hôtel-Dieu Grace Healthcare

April 5, 2022

Summary: This decision and related PHIPA Decision 176 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 Hôtel-Dieu Grace Healthcare (HDGH), as well as accesses by an HDGH agent to a record in the custody or control of the other hospital, Windsor Regional Hospital – Ouellette Campus. In this decision, the adjudicator finds that the accesses at issue 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 HDGH 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 to help improve HDGH's 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), 17, 29, 30, 36(1)(c)(iii), 36(1)(g), 37(1)(a), 37(1)(d), 37(2), and 39(1)(d); *Quality of Care Information Protection Act, 2016*, SO 2016, c 6, Sch 2.

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

BACKGROUND:

[1] This decision and related PHIPA Decision 176 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 Hôtel-Dieu Grace Healthcare (HDGH). A related complaint was made against Windsor Regional Hospital—Ouellette Campus (WRH). 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. I considered, but declined, HDGH's request to have the two complaints addressed together at the review stage. Although the complaints involve some of the same accesses, I decided that separate reviews are appropriate, given there are different respondents and some issues specific to each complaint. However, in view of the fact some of the accesses involve both hospitals, I shared relevant portions of HDGH's and WRH'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 HDGH, as well as the access by an HDGH agent to a record in the custody or control of WRH. (I discuss the meanings of the terms "agent" and "custody or control," below.) The related PHIPA Decision 176 addresses the allegations concerning accesses to patient records in the custody or control of WRH, and accesses by WRH agents to records in the custody or control of HDGH. 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 find that the accesses at issue were made in accordance with *PHIPA*. I also find that HDGH 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 for consideration by HDGH in respect of its policy on the use of personal health information for quality assurance purposes.

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 HDGH.

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 HDGH and WRH. 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, HDGH and WRH provided useful background about the relationship between the two hospitals, which I summarize as follows.

[11] HDGH and WRH 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 HDGH and WRH. 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, HDGH and WRH 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. Both hospitals have implemented a new EMR called Cerner, which is accessible to users at both HDGH and WRH. I discuss the new

EMR later in this decision.)

[15] As I discuss in more detail below, HDGH and WRH 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 HDGH, 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 HDGH (based on the patient's receiving care at HDGH), while other records originated from WRH (based on the patient's receiving care at WRH). For ease of reference, in this decision I will refer to the former records as "HDGH records," and the latter records as "WRH 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 HDGH are certain accesses made by an individual at HDGH to several HDGH records and to one WRH record. Also at issue are certain accesses to HDGH records by two different individuals at WRH.

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

- 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);

- Access (occurring the same day, seven days after the patient's death) by the same HDGH doctor to various HDGH records (a clinical note and a crisis service note authored by another physician at HDGH; and a clinical note authored by the HDGH doctor himself);

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

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

[20] 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 176. 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).

[21] For the reasons set out below, I conclude that these accesses to the patient's records were made in compliance with *PHIPA*. I also find that HDGH 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 conclude the review without issuing any order against HDGH. However, I make some comments for consideration by HDGH to improve its privacy policy as it relates to the use of personal health information for quality assurance purposes.

PRELIMINARY MATTERS:

[22] 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.

[23] 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.

Health information custodians and agents

HDGH and WRH are health information custodians

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

[24] There is no dispute, and I find, that HDGH 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 WRH that WRH 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

[1] For reasons I explain further below, it is not possible to identify which records were accessed by WRH Employee B on this date.
[2] More particularly, "the person who operates" HDGH is a health information custodian under this section of *PHIPA*.

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 HDGH and WRH.

[25] These rules also apply to agents of HDGH and WRH. 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)].

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

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

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

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

[28] 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 HDGH and WRH at the relevant times.

[29] 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.

[30] 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 an outpatient clinic note prepared by an HDGH agent at HDGH, and uploaded to Solcom by HDGH, is an "HDGH

[3] 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). See the discussion in PHIPA Decision 110.

record." Similarly, a discharge summary created by a WRH agent at WRH, and then uploaded to Solcom by WRH, is a "WRH record."

[31] 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.[4] When one 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

[32] 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.[5]

- The same transaction involves a "disclosure" of personal health information by the hospital that contributed the record to the shared EMR.[6]

- 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.[7]

[33] 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.

---

[4] PHIPA Decisions 102 and 110.

[5] 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[.]"

[6] 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[.]"

[7] 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.

Any collection, use, or disclosure must comply with PHIPA

[34] 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 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*.

[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.

[36] HDGH does not claim that the accesses at issue were made with consent from the appropriate person. Instead, HDGH 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.

[37] With this background in mind, I now consider HDGH's responsibilities in respect of each of the accesses at issue in this complaint. (I address WRH's responsibilities in respect of the common transactions in the related PHIPA Decision 176.)

ISSUES:

A. Did the HDGH doctor's collection, and use, of the patient's personal health information comply with *PHIPA*?

B. Did HDGH's disclosure of the patient's personal health information to WRH Employees A and B comply with *PHIPA*?

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

DISCUSSION:

A. Did the HDGH doctor's collection, and use, of the patient's personal health information comply with *PHIPA*?

[38] Under this heading, I will consider 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.

[39] As explained above, this access involves a "collection" of personal health information by the HDGH doctor, because the record he accessed originated from WRH. (The related PHIPA Decision 176 addresses the aspect of this same transaction that constitutes a "disclosure" of the same information by WRH to the HDGH doctor.) I must also consider the appropriateness of the HDGH doctor's subsequent "use" of the personal health information he collected from WRH.

[40] I will also consider under this heading the HDGH doctor's accesses on the same date to several HDGH records in Solcom. These records are: a mental health clinical note and a crisis service note authored by another physician at HDGH; and a clinical note authored by the HDGH doctor himself. These were "uses" by the HDGH doctor of personal health information in the custody or control of HDGH.

[41] Therefore, the issue under this heading is whether the collection, and use, of personal health information by the HDGH doctor complied with *PHIPA*. For the reasons that follow, I find that these actions complied with *PHIPA*.

[42] HDGH provides context for these transactions by explaining the HDGH doctor's various roles at the hospital. The doctor treats patients in the General Psychiatry Clinic (the clinic) in the hospital's Transitional Stability Centre, a crisis wellness centre. In this role, the HDGH doctor had provided health care to the patient. 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.

[43] HDGH submits that in this context, the HDGH doctor had legitimate reasons for accessing the patient's records after learning of the patient's death. His purpose was to assess the quality of the care that he and others had provided to the patient. The doctor's interest was both as a former care provider, with professional obligations to assess the care he had provided for quality improvement and learning purposes,[8] and as an administrator of the clinic, with duties to maintain and improve overall quality standards at the clinic.

[44] The complainant says he believes the HDGH doctor had honest and sincere motivations in accessing the patient's records after the patient's death. However, the complainant notes that the doctor had discharged the patient from his care several months before the patient died, and there was thus no active care relationship between them when the doctor accessed the patient's records. The complainant questions why HDGH would condone accesses occurring after a care relationship has ended, and he seeks changes to HDGH's policy in this regard.

[45] The complainant also questions why the HDGH doctor accessed particular HDGH records, and not others (such as the patient's records from the hospital's Transitional

[8] HDGH refers to guidance provided by the College of Physicians and Surgeons of Ontario to its member physicians, including on the need for physicians to maintain quality care through self-learning and self-regulation.

Stability Centre), if the doctor's purpose was to assess the quality of care.

[46] I find that the doctor's collection and use of the patient's personal health information complied with *PHIPA*. This is because I am satisfied these actions were undertaken for authorized purposes relating to quality of care and quality improvement under *PHIPA*.

[47] First, I accept that the HDGH doctor's collection of the WRH record (a discharge summary) was 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[.]

[48] As a hospital, HDGH 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). I am satisfied that the HDGH doctor's 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 the *Quality of Care Information Protection Act, 2016*, to provide quality health care.

[49] The collection was also authorized under section 36(1)(g) of *PHIPA*. This section permits a custodian (or, in this case, an agent 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 176, I find that in this same transaction, WRH was authorized to disclose this personal health information to the HDGH doctor under section 39(1)(d) of *PHIPA* (disclosure to another custodian to improve or maintain quality of care). As a result, the corresponding collection of this same information by the HDGH doctor complied with section 36(1)(g).[9]

[50] I further find that the subsequent use of the WRH record by the HDGH doctor

---

[9] HDGH reports that the HDGH doctor already had a copy of the WRH record in his possession, because he was sent a copy by the physician at WRH. On the date of his access, the HDGH doctor was not in his office to examine his own copy, so instead he accessed the record in Solcom. On this basis, HDGH argues that the HDGH doctor made a "technical, not substantive," collection of the WRH record; it also argues that the initial collection was made on the basis of assumed implied consent. (I acknowledge here that the complainant takes issue with the WRH physician's having sent a copy of the record to the HDGH doctor. That matter is outside the scope of this review under *PHIPA*.)
PHIPA does not distinguish between "technical" and "substantive" collections. In any event, whether the transaction is analyzed as a collection and then a use (as I have done here), or simply as a use, I would find the HDGH doctor's access was authorized under *PHIPA*.

was authorized by section 37(1)(a) of *PHIPA*, which permits the use of personal health information for the purposes for which the information was collected.[10] Having collected the record for quality of care and risk management purposes, and in the absence of any evidence to the contrary, I accept that the doctor then used it for that same purpose.

[51] The doctor's use of the WRH record was also authorized under section 37(1)(d),[11] which permits the use of 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." This section also authorized the HDGH doctor's use of HDGH records for the same purposes. Taking into consideration the circumstances of the patient's death and the HDGH doctor's roles within the hospital, I accept that the doctor's use of the patient's records was for quality of care purposes within the meaning of section 37(1)(d).

[52] I am mindful of the complainant's concern that there could be improper accesses by care providers to patient records after the care relationship has ended. There is no evidence that this occurred here. The text of section 37(1)(d) does not limit uses under this section to circumstances where personal health information is relevant to an active care relationship, and I see no reasonable basis for reading in such a requirement. For instance, it is not hard to imagine circumstances in which examining past care relationships could be relevant to the risk and error management activities contemplated by section 37(1)(d). Furthermore, HDGH's policy concerning such uses does not prohibit its agents from using the personal health information of former patients for quality assurance purposes,[12] and *PHIPA* does not require HDGH to impose such a condition on this use. Given this, there is no support for the claim that the HDGH doctor's use of the patient's records for this authorized purpose after the patient's death reflects a gap in the hospital's policy.

[53] I have also considered the complainant's concerns about the particular records the HDGH doctor accessed for these purposes. 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.

[54] There is no claim by the complainant nor any evidence before me to suggest that the HDGH doctor collected and used more personal health information than was reasonably necessary for the quality assurance purposes outlined above, or otherwise contravened section 30. In fact, the complainant's concern is slightly different, in that he appears to suggest the doctor ought to have accessed more records for this purpose than he actually did. This is not a basis on which to find a violation of the data minimization principle in section 30. It also does not, in the circumstances, detract from

[10] Section 37(2) of *PHIPA* permits a custodian's agent to use personal health information for the purposes authorized in section 37(1) of *PHIPA*.
[11] In combination with section 37(2), as noted above.
[12] HDGH provided relevant excerpts of its privacy policy, which were shared with the complainant.

my finding, above, that the HDGH doctor used the records he did for quality assurance purposes in accordance with *PHIPA*.

[55] I conclude that the HDGH doctor collected and used personal health information in compliance with *PHIPA*.

B. Did HDGH's disclosure of the patient's personal health information to WRH Employees A and B comply with *PHIPA*?

[56] At issue under this heading are accesses by two employees of WRH to certain HDGH patient records in Solcom.

[57] 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.

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

[59] As explained above, these accesses involve "disclosures" of personal health information by HDGH to agents of WRH, because the records at issue originated from HDGH. (The related PHIPA Decision 176 addresses the aspects of these same transactions that constitute "collections" by WRH (through its agents) of this information from HDGH.)

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

[61] 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 disclosures

considered under this heading.

[62] First, the disclosure was made to agents of WRH, 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).

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

[64] 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, WRH), either to the patient, or to other individuals to whom WRH provides similar health care.

[65] On this issue, both HDGH and WRH provided relevant background about the roles of WRH Employees A and B at the time of their accesses.

[66] At the relevant time, 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 WRH, and performing quality assurance duties, including reviews under the *Quality of Care Information Protection Act, 2016* (*QCIPA*).[13] WRH explains that at the time of WRH Employee A's access to HDGH records (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 that occurred.

[67] WRH Employee B also had patient relations responsibilities at WRH, in her role as a hospital Patient Representative. WRH 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 advises 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.

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

[69] 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

[13] 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*).

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.

[70] Considering the circumstances of the patient's death and the WRH employees' roles at the hospital, I am satisfied that HDGH's disclosure to WRH (through its agents) met the requirements of section 39(1)(d). I accept that the purpose of the disclosure by HDGH (and the collection by the WRH agents) was to investigate the circumstances of the patient's death and to respond to the concerns of the patient's family, which I find to be quality of care activities within the meaning of section 39(1)(d). The broader purpose of these activities was to improve or maintain the quality of mental health care provided by WRH to its patients. (For related reasons, I find in PHIPA Decision 176 that the WRH agents' corresponding collection of HDGH records also complied with *PHIPA*.)

[71] The complainant was invited to respond to both HDGH's and WRH's representations on this topic. In his responding representations, the complainant questions why WRH did not invite HDGH to participate in its *QCIPA* review, and why HDGH did not conduct its own *QCIPA* review.

[72] It is clear from these and other comments made in both complaints that the complainant has serious concerns about both hospitals' *QCIPA* processes. However (and as I discuss in more detail in the related PHIPA Decision 176 against WRH), these broader concerns about the *QCIPA* process that occurred are outside the scope of my review under *PHIPA*. Specifically, in deciding whether HDGH's disclosure to WRH complied with *PHIPA*, I do not view as relevant the fact HDGH did not conduct its own *QCIPA* review. More generally, I note that the provisions in *PHIPA* that permit access for quality of care purposes are not limited to circumstances in which a custodian conducts a *QCIPA* review.

[73] Lastly on this topic, as noted above, the collection and use of personal health information must comply with section 30 of *PHIPA*.

[74] As described above, HDGH's disclosure to WRH Employee A 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.

[75] With respect to HDGH's disclosure to WRH Employee B, WRH (which conducted the audit) states that it is unable to identify precisely which HDGH records were collected by WRH Employee B (and thus disclosed by HDGH) 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 or 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.

[76] The complainant made no comment on WRH's statements on this issue in the

other complaint. There is no claim by the complainant nor any evidence before me to suggest that WRH Employee B's collection (and HDGH's corresponding disclosure) involved more personal health information than was reasonably necessary for the purposes outlined above, or otherwise contravened section 30. In the circumstances, I have no reason to believe the disclosure did not comply with *PHIPA*.

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

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

[78] *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.

[79] 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.[14]

[80] 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)].

[81] Custodians must also 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.[15] Custodians remain responsible for any personal health information handled on their behalf by their agents.[16]

[82] During the course of the review, the IPC asked HDGH to provide details of the administrative, technical, and physical safeguards in place to protect the security of personal health information in the shared EMR. Because WRH also plays a role in ensuring the security of the shared system, its representations on this topic (filed in the related complaint) are also relevant.

---

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

[83] HDGH and WRH are parties to a data sharing agreement in respect of the shared EMR, a copy of which I received. Staff at both hospitals with access to the shared system are also required to sign the confidentiality agreements of each hospital. HDGH explains that professional staff (like the HDGH doctor) are required to sign HDGH's confidentiality agreement as part of the initial credentialing and orientation process, and afterward on a yearly basis as part of the annual re-application for privileges. Among other things, the confidentiality agreement requires staff to confirm their understanding of and consent to act in accordance with hospital by-laws, rules and regulations, and hospital policies.

[84] HDGH confirmed that the HDGH doctor (whose accesses are addressed in this complaint) was covered by a valid confidentiality agreement at the relevant time under review. Professional staff are also required to undergo regular privacy training, including on the appropriate use of personal health information for quality assurance purposes.

[85] HDGH provided copies of relevant hospital policies. This includes its privacy policy, which addresses accesses for quality assurance purposes. The policy indicates that in order to use personal health information for quality assurance or quality improvement purposes, HDGH agents must have the knowledge and permission of management, and must document the quality assurance purpose of the access in the patient's record in the EMR.

[86] However, HDGH explains that physicians are not subject to either of these requirements in the case of accesses for quality assurance purposes. This is based on HDGH's determination that physicians are already subject to professional duties to use personal health information appropriately for quality of care purposes. HDGH also says it is unnecessary for treating physicians to document their quality assurance accesses to the records of patients they have cared for, since the care relationship would be evident from the record itself. During the review, the hospital advised that it would be amending its privacy policy to make clear that physicians do not need to document the reason for their accesses to a patient's record if they have treated the patient and are carrying out their duties and responsibilities in compliance with the hospital's professional by-laws.

[87] In my view, the more prudent approach would be to apply consistent documentation requirements on all hospital agents, including physicians, in the case of accesses for quality assurance purposes. The burden on physicians to document the quality assurance purpose of a given access would be minimal, while extending the documentation requirement to all agents would provide a simple check against unauthorized access. It would also promote the message that all agents are expected to take steps to protect the security of patient information. Clear and consistent documentation of the purpose of access would also facilitate audits. I observe that WRH requires professional staff (such as doctors) to document in the shared EMR any accesses made for quality assurance purposes. I encourage HDGH to consider amending its policy for the reasons given above, and for consistency with WRH's practices.

[88] Since the time of the accesses at issue, and for reasons unrelated to this complaint, HDGH and WRH adopted a new shared EMR system, called Cerner. All users received training on the new system, and were required to complete additional privacy and security training before being granted access to the new system. All staff, including physicians, are required to complete the privacy and security training on a yearly basis.

[89] In the related PHIPA Decision 176, I describe in more detail some features of the new Cerner system that will help address additional issues that arose in the complaint against WRH. These features include: a more convenient log-in and log-out system for EMR users; automatic log-out after five minutes of user inactivity; and a more robust auditing feature. The new system's regular auditing features, including targeted and random audits, is a key technical safeguard against unauthorized accesses in the EMR.

[90] The hospitals also describe other technical safeguards in place, including unique staff passwords and user IDs, and strong encryption, firewalls and virus scanning provided by the hospitals' shared service provider. I was also provided with 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.

[91] The hospitals advise 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,[17] 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 HDGH, WRH, and the other participating custodians to IPC guidance on this topic, including particularly PHIPA Decision 102.[18]

[92] Taking into account all the above, I am satisfied that HDGH complied with its obligations under section 12(1) to take reasonable steps to protect personal health information in its custody or control. I am also satisfied it responded adequately to the complaint. Before and during this complaint process, HDGH took steps to investigate the accesses identified by the complainant, including by consulting with WRH, and to communicate the results to the complainant. Both HDGH and the complainant have cooperated fully in the complaint process.

[93] For all these reasons, I find that HDGH complied with *PHIPA*. I dismiss the

---

[17] https://www.weoht.ca/aboutOHTs.

[18] Also PHIPA Decisions 62 and 110; also 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.

complaint.

NO ORDER:

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

Original Signed by: April 5, 2022

Jenny Ryu
Adjudicator