Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 110

Files HR16-73 and HR16-131

Trillium Health Partners

Two physicians

February 18, 2020

Summary: This decision sets out the adjudicator's findings following self-initiated reviews under section 58(1) of the *Personal Health Information Protection Act, 2004* (*PHIPA*) of two separate privacy breach incidents reported to this office by Trillium Health Partners (THP), a multi-site hospital. Each incident involved remote (off-site) accesses to THP's Electronic Medical Records (EMR) system from the private practice office of a THP physician. In each case, the accesses at issue were made by, or under the EMR credentials of, an employee of the physician's private practice who had been granted permission by THP to access THP's EMR for the purpose of assisting in the provision of health care to the physician's private practice patients.

The adjudicator finds that both THP and remote access users of THP's EMR (including the physicians and their employees) have responsibilities under *PHIPA* to protect personal health information in THP's EMR, and that the confidentiality of this information was breached through numerous instances of snooping by the physicians' private practice employees. The transactions at issue are "disclosures" by the health information custodian THP, and "collections" of the same information by agents of the physicians, as the physicians are themselves health information custodians in respect of their private practices. Many of these transactions were made in contravention of *PHIPA*. The adjudicator considers the circumstances that gave rise to these breaches, and the steps taken by the respondents THP and the physicians since that time. She concludes that the respondents have taken reasonable steps to contain and to respond to the privacy breaches, and to implement changes to their information practices to comply with their obligations under *PHIPA*. While the adjudicator makes a number of comments for the benefit of the respondents, no order is issued in the circumstances.

Statutes Considered: *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Sch A (as amended), sections 2 (definitions), 3(1), 10(1), 10(2), 12(1), 12(2), 17, 20(2), 29 and 58(1).

Orders and Decisions Considered: Orders HO-002, HO-010 and HO-013, and PHIPA Decisions 62 and 102.

INTRODUCTION:

[1] This decision sets out my findings following my review under section 58(1) of the *Personal Health Information Protection Act, 2004 (PHIPA*) of two separate privacy breach incidents reported to this office by Trillium Health Partners (THP), a multi-site hospital. These incidents arose from the actions of two different individuals who remotely accessed personal health information of THP patients in THP's Electronic Medical Records (EMR) system. THP reported its concerns that these individuals had inappropriately viewed the personal health information of a number of patients in its EMR without authorization and in contravention of *PHIPA*.

[2] Under section 58(1) of *PHIPA*, the Office of the Information and Privacy Commissioner (IPC) may, on its own initiative, conduct a review of any matter if it has reasonable grounds to believe that a person has contravened or is about to contravene a provision of *PHIPA* or its regulations. While I conducted separate reviews of the two incidents, I address them together in this decision because they raise similar issues concerning the obligations under *PHIPA* to protect the confidentiality and security of patient personal health information.

[3] In this decision, I find, among other things, that both THP and remote access users of THP's EMR (which includes the physicians and their employees) have responsibilities under *PHIPA* to protect patient information in the EMR, and that the confidentiality of this information was breached through numerous instances of snooping in the EMR by employees of private practice physicians. During the course of these reviews, the respondents THP and the physicians cooperated with this office in thoroughly investigating these incidents, and in identifying and addressing deficiencies in their practices that may have played a role in enabling these breaches of patient privacy. In the discussion that follows, I conclude that through these measures and others, the respondents have taken reasonable steps to contain and to respond to the privacy breaches, and to implement changes to their practices to comply with their obligations under *PHIPA*. I conclude that no order is required in the circumstances.

BACKGROUND

[4] The incidents under review involve remote (off-site) accesses[1] to THP's EMR by employees of "credentialed" physicians, meaning physicians who have privileges to practise medicine at THP.[2] THP explains that it grants remote EMR access to credentialed physicians and, upon request, to private practice employees of those physicians, as part of a service offered to credentialed physicians who also treat patients in their own private practices outside THP. Later in this decision, I will examine this arrangement in more detail to address the implications under *PHIPA* for the various parties involved.

[5] In each of the two incidents under review, a THP-credentialed physician had sought and been granted permission from THP for an employee of his private practice to remotely access THP's EMR for the purpose of assisting the physician in the provision of health care to patients in the context of his private practice. The employees accessed THP's EMR for such purposes as retrieving patient health records and ensuring the correct identification of patients for OHIP billing purposes. THP explains that records of the care a patient receives at THP can be relevant to the care that a private practice physician provides to that same patient, whether or not that physician also cares for the patient at THP. These records can include, for example, lab results or imaging data, or records of the patient's visits to THP departments that did not involve the physician but that are nonetheless relevant to the care he provides to the patient in his private practice.

[6] The two private practice physicians involved in these incidents are respondents in these reviews. However, I have not named them or their employees in this decision, as doing so could lead to the identification of individuals whose personal health information is at issue. For ease of reference, I will refer to these parties as Physician A and Employee A, and Physician B and Employee B.[3]

[7] I begin by describing the events that led to THP's privacy breach reports to the

---

[1] In this decision, I use the terms "access" and "view" colloquially, in the manner they are used by the parties, to describe the transactions in the EMR system that are at issue in these reviews. I distinguish this colloquial use from the meaning of these terms as they appear elsewhere in *PHIPA.* See also footnote 10.

[2] Credentialing refers to the process in the *Public Hospitals Act* in which Ontario hospitals permit some health professionals such as physicians to become professional staff members with privileges to provide health care at the hospitals. THP provided detailed information about its credentialing process, which I have not reproduced here.

[3] To the extent that I examine the conduct of Employee A and Employee B in this decision, this is based on the evidence and submissions provided to me by THP and the physicians, and is ancillary to my review of the systemic issues arising from remote accesses to THP's EMR system—and, namely, of whether the respondents THP and Physicians A and B complied with their obligations under *PHIPA* in these EMR transactions.

IPC.

File HR16-73 (Respondents THP and Physician A)

[8] In 2016, THP received a complaint from an individual indicating that a family member may have inappropriately viewed her records of personal health information. Upon investigation, THP determined that an administrative assistant at the private practice office of a THP-credentialed physician (Employee A of Physician A) had viewed the complainant's records in THP's EMR.

[9] THP's audit of Employee A's accesses to the complainant's records in THP's EMR indicated that Employee A had viewed the complainant's records on numerous occasions during a period of about 4.5 years preceding the date of the complaint. THP immediately suspended Employee A's access to the EMR and notified Physician A of its investigation. THP also reported the privacy breach to the IPC.[4]

[10] THP then broadened its investigation of Employee A's accesses in the EMR, with the assistance of Employee A, Physician A and another physician who shared office space with Physician A in a medical office building located near one of THP's hospital sites. The other physician is also a THP-credentialed physician. THP later determined that a significant number of THP-credentialed physicians have private practice offices in this building. (As will be seen below, the related file HR16-131 involves other credentialed physicians with offices in this same medical building.)

[11] THP's investigation of Employee A's activity in the EMR revealed that Employee A had inappropriately viewed the personal health information of 15 patients with whom Employee A has familial or other relationships. When presented with these findings, THP reports that Employee A readily acknowledged that she had viewed these patients' records (or, where she did not recall, that she had likely viewed these records) for purposes unrelated to her job duties. Employee A explained that some of these accesses had been made with the permission of or at the request of the patient, and that others had been made for reasons of care and compassion.

[12] THP sent notification letters to these patients (in one case, to the estate of a deceased patient), informing them that their records of personal health information had been inappropriately accessed by an employee of Physician A through THP's computer systems. In these letters, THP provided each patient with details of the privacy breach, including the type of information accessed, the number of accesses and the period of time during which the accesses occurred. THP also described the steps that it had taken on discovering the privacy breach, including the immediate and permanent suspension

[4] The original complainant also filed her own privacy complaint with the IPC about this matter. That complaint file addressed specific issues arising from the complainant's allegations about her family member's activity in her health records, and was resolved at the intake stage of the IPC's process.

of the employee's access to THP computer systems (including its EMR), and its reporting of the privacy breach to the IPC.

[13] One of the notified individuals is the mother of Employee A. This notified individual contacted THP to report that she had given Employee A permission to view her health records. The mother takes the position that her privacy was not breached by Employee A. THP later heard from two additional individuals who are friends of Employee A, and who also take the position that Employee A accessed their records with permission.

[14] THP's investigation also initially indicated that Employee A may have inappropriately viewed the records of a significant number of individuals with whom she does not have personal relationships. These individuals did not initially appear to be patients of Physician A, raising questions about the purpose of Employee A's accesses to their records.

[15] However, after further analysis and investigation by THP, THP determined that the vast majority of these accesses had been made for health care–related purposes. For example, THP learned that Employee A also worked for the physician who shared office space with Physician A, and regularly accessed THP's EMR on behalf of this other physician. As noted above, this other physician is himself a THP-credentialed physician with his own private practice. THP deemed Employee A's accesses to the records of patients of this other physician in the EMR to be legitimate accesses by Employee A on behalf of the other physician, in order to assist in the provision of health care to private practice patients of that physician.

[16] THP also learned that other employees of Physician A or the neighbouring physician regularly used Employee A's user IDs and passwords to access THP's EMR for similar purposes. THP concluded that a significant number of patients whose records had been accessed using Employee A's EMR credentials had a documented health care relationship with one or the other physician. THP determined that these accesses were also made for legitimate health care purposes.

[17] By the end of THP's investigation, there remained 249 patients whose records had been accessed by Employee A (or by using Employee A's user IDs and passwords) in relation to whom THP could not make definitive findings on the legitimacy of access. These are patients who have no documented relationship with either Physician A or the other physician. Based on its assessment of all the evidence, however, THP takes the position that these were likely authorized accesses for health care purposes.

[18] Among other reasons, THP observes that none of these individuals has a personal connection to Employee A, and that Employee A has willingly acknowledged having inappropriately accessed (or having likely accessed) the records of individuals known to her. This includes some individuals that THP had not already identified through its own investigation. Employee A maintains, however, that she would not have accessed the records of individuals whom she does not know without an authorized

purpose. Based on all the circumstances, THP states that it finds Employee A's assertion to be highly credible.

[19] Moreover, THP submits, the inability to identify the precise reason for each of the remaining accesses is not evidence that they were unauthorized accesses under *PHIPA*. Many of the remaining accesses have connections to ophthalmology (the field in which Physician A practises), which suggests a legitimate health care–related purpose for the access. THP also observes that some legitimate accesses in the EMR may (inaccurately) appear to be unauthorized accesses, for various reasons. For example, where a patient referral to a physician is refused by the physician or the individual fails to attend, the individual is not documented as a patient of the physician, in spite of the legitimate health care purpose for access to that record.

[20] THP also notes that human error, such as imperfect record-keeping of patient visits and accidental accesses to the wrong patient record, can generate entries that appear to be unauthorized accesses. Furthermore, despite the substantial publicity that this breach incident has received—through THP's notifications to affected individuals (which led to THP's being contacted by some additional individuals that THP had not itself identified during its investigation), and through media attention to a legal proceeding commenced by the original complainant (the family member of Employee A)—THP reports that it has not received any additional privacy breach complaints from members of the public.

[21] In all, considering the passage of time and the difficulty of pinpointing the purpose of single accesses several years after the fact, THP submits that it is not unreasonable that its comprehensive audit (spanning a 17-year period) generated some accesses for which THP is unable to determine the precise reason. Nonetheless, based on all the evidence, THP concludes that the accesses to the records of these remaining 249 patients were more likely than not made for the purpose of providing health care. Based on this assessment, THP did not provide notice of a privacy breach to these 249 patients.

[22] During the course of the IPC's investigation into this matter, Physician A confirmed that he had dismissed Employee A as a consequence of the privacy breach.

File HR16-131 (Respondents THP and Physician B)

[23] Shortly after it became aware of the privacy breach incident described above, THP conducted a routine random audit of accesses in its EMR that revealed another potential privacy breach. This breach involved a secretary employed by another THP-credentialed physician who also operates his own private practice (Employee B of Physician B). THP's random audit indicated that Employee B may have inappropriately accessed the records of five individuals in THP's EMR from Physician B's private practice office. As in the incident described above, THP had granted the physician's employee permission to access THP's EMR in order to assist the physician in the provision of health care to patients of his private practice.

[24] Upon learning of the audit results, THP immediately and permanently terminated Employee B's access to THP's EMR. THP began an investigation into all Employee B's activity in the EMR since 2007, the year she was first given permission to access the EMR on Physician B's behalf. THP also notified the IPC of this second privacy breach incident.

[25] Although Employee B initially met with THP to discuss some of the audit results, she later refused any further involvement in THP's investigation. Despite this, with the assistance of Physician B and a third-party investigator, THP was able to make determinations about the vast majority of Employee B's accesses in the EMR.

[26] Specifically, at the conclusion of its investigation, THP determined that Employee B had inappropriately accessed (or had likely inappropriately accessed) the records of approximately 50 individuals.[5] Some of these accesses involved individuals who had been admitted to mental health services (which has no apparent connection to Physician B's endocrinology practice), and whose records had been accessed in close succession. Other accesses involved individuals with the same surname or former surname as Employee B, or who have some other social connection to Employee B, where there is no apparent patient relationship to Physician B that would suggest a legitimate health care purpose for the access. (As discussed below, there is also no apparent patient relationship to any other THP-credentialed physician with a private practice office located in the same medical building.) For these cases, THP concluded that the accesses were either highly likely to be unauthorized, or else were "fully unexplained." As a result, during its investigation and through the course of this review process, THP notified each of these affected individuals.

[27] By contrast, THP concluded that other accesses identified during its audit were more likely than not authorized accesses made for legitimate health care purposes. These include accesses to the records of patients who may have received referrals to Physician B, but who ultimately received endocrinology care from another physician (and thus had no documented relationship with Physician B in the EMR). THP also concluded that very brief accesses (to records of patients with no documented relationship with Physician B or other THP-credentialed physician, as described below) were more likely than not accidental or inadvertent accesses, rather than intentional unauthorized breaches.

[28] During its investigation, THP learned that Employee B had worked for other THP-credentialed physicians with private practice offices in the same medical building as

---

[5] This figure excludes a number of individuals who were initially notified by THP of potential unauthorized accesses to their records in THP's EMR, but who were later identified as patients of Physician B (such that the accesses to their records were deemed to have been legitimate accesses for health care purposes). THP later sent these individuals follow-up letters correcting and apologizing for the error.

Physician B. (As noted above, Physician A also has a private practice office in this medical building.) THP also learned that Employee B may have shared her EMR user IDs and passwords with employees of other private practice offices operating at the same building.

[29] Based on this information, THP examined Employee B's other accesses to determine whether they could be linked to private practices located in the medical building. THP contacted each of the 83 physicians with offices in the building, and determined that 65 of these physicians are THP-credentialed physicians who, like Physician A and Physician B, have permission from THP to access THP's EMR to view medical records of THP patients whom the physicians treat in their private practices.

[30] Through its investigation, THP learned that three different THP-credentialed physicians with private practice offices in the building had employed Employee B at different times, and that it was possible she had also done work for two additional private practice offices. For THP, these findings confirmed the legitimacy of Employee B's accesses to the records of patients connected to the other physicians for whom Employee B had worked. They also strongly suggested that Employee B's accesses (or accesses made using her user IDs and passwords) to the records of patients of other credentialed physicians with private practice offices in the same building may also have been made for legitimate health care purposes. For example, where accesses were limited to health records relevant to the practice of the physician to whom the patient was connected, THP concluded that they were most likely made for authorized purposes—even where THP was unable to confirm that Employee B had worked for that physician (as in the case of one private practice that had since closed).

[31] Furthermore, as in the other privacy breach incident, THP notes the difficulty of determining the precise reason for discrete accesses made during the extended time period covered by its audit. THP also observes that despite the number of notices given in this matter (and the substantial publicity and coming forward of new affected parties arising from the related matter), THP did not receive any additional inquiries from patients about potential inappropriate accesses to their records.

[32] In these circumstances, THP submits that it has likely identified most or all instances of unauthorized access, and has provided notice in accordance with its obligations under *PHIPA*. In particular, THP notified all the individuals for whom there is a high likelihood of unauthorized access (namely, those patients with surname and other social connections to Employee B), and those for whom the purpose of access remains "fully unexplained" despite THP's thorough investigation (for example, those individuals who do not appear to have a health care connection to Physician B or other THP- credentialed physician with a private practice in the same medical building).

[33] For the remainder of the accesses, THP submits that the evidence does not support a finding of an actual or probable breach of *PHIPA*. For these remaining 260 patients, THP believes that a full assessment of the entire factual scenario suggests there were legitimate health care purposes for the accesses, or that the accesses were

accidental (given the brevity of access), rather than intentional unauthorized accesses. Based on this assessment, THP has not notified these 260 individuals.

[34] During the IPC review process, Physician B informed the IPC that he had dismissed Employee B.

IPC investigation and review

[35] In response to the privacy breach reports from THP, the IPC opened two separate investigation files. During these investigations, the IPC sought and received information from THP, including about the discovery of the breaches; THP's and the physicians' actions in response to the breaches; the relationship between THP, the physicians and the private practice employees of the physicians; and the administrative, technical and physical safeguards in place to protect the security of patient information in the EMR.

[36] At the conclusion of the IPC's investigation, there remained a number of unresolved issues in both files, including whether THP or the physicians (or both) are "health information custodians" in respect of the information accessed in THP's EMR, and whether notice of the privacy breaches had been provided in accordance with *PHIPA*. Given this, the files were transferred from the investigation stage to the adjudication stage of the IPC's process.

[37] I decided that there were reasonable grounds to conduct reviews of both matters under section 58(1) of *PHIPA*. As part of my reviews, I sought representations on the issues arising from these incidents from the respondent THP, as well from Physician A and Physician B, whom I added as respondents given their central roles in these matters. In addition, because the broader issues in these reviews may have impacts on other hospitals in Ontario that maintain and grant user access to EMR systems, I decided to notify and to invite submissions on the issues from the Ontario Hospital Association, which provided representations on behalf of its member hospitals. The respondents THP and the physicians also provided representations for my consideration.

[38] In the discussion that follows, I find that there were some failures on the part of THP and the physicians to comply with *PHIPA* at the time of the incidents, which may have contributed to enabling the privacy breaches under review. I also find, however, that the respondents have taken reasonable steps to address the breaches, both through the containment measures taken immediately after their discovery, and through some broader changes implemented by the respondents since that time to ensure better protection of patient privacy and the security of EMR information. While I conclude that no order is necessary in the circumstances, I provide some comments on additional best practices that will assist the respondents in complying with their obligations under *PHIPA*.

DISCUSSION:

[39] *PHIPA* sets out rules for the collection, use and disclosure of personal health information to protect the confidentiality of that information and the privacy of the individuals to whom that information relates, while at the same time facilitating the effective provision of health care (section 1). *PHIPA* achieves these purposes by, among other things, imposing duties on health information custodians to protect personal health information in their custody or control, and by establishing independent oversight powers of the IPC to address contraventions or potential contraventions of *PHIPA*.

[40] All the parties agree that the records of patient information in THP's EMR are records of "personal health information" as that term is defined in *PHIPA* (section 4), and that *PHIPA* governs the activities of the respondents THP and the physicians in relation to the EMR transactions under review.

[41] At the outset of the review process, however, there was some dispute about the specific roles and responsibilities of the parties in these transactions, particularly as they relate to the activities of the physicians' private practice employees. This raises the key issue of who is the "health information custodian" in respect of the personal health information at issue in these reviews. Identifying the roles of the various parties in the EMR transactions is a key first step in determining who is responsible under *PHIPA* for such duties as implementing information practices that comply with *PHIPA*, providing adequate training to EMR users, and notifying those individuals whose personal health information may have been accessed without authority in the EMR.

[42] As will be seen below, I conclude that each of THP, Physician A and Physician B is a health information custodian in relation to the EMR transactions under review, and, accordingly, that each had responsibilities under *PHIPA* to safeguard the personal health information at issue. I then consider whether the respondents were meeting their responsibilities under *PHIPA* at the time of the incidents under review, and whether they have addressed any deficiencies in their practices identified through these reviews.

Health information custodians and agents

THP is the health information custodian of the personal health information in the EMR

Each physician is a health information custodian in respect of his own private practice, and each employee is an agent of the responsible physician

[43] During the review process, I asked the parties for their views on who is the health information custodian in respect of the personal health information at issue in these reviews.

[44] I noted that in each case, a THP-credentialed physician was granted permission by THP to access THP's EMR remotely from his private practice office, for the purpose of providing health care to patients in the context of that private practice. Each physician had also obtained permission for the employee of his private practice to remotely access the EMR for the purpose of assisting in the provision of health care to his private practice patients. The EMR transactions that are at issue in these reviews were made under two private practice employees' user IDs and passwords for accessing the EMR.

[45] When THP or the physicians (in the context of their private practices) have custody or control of personal health information in connection with the performance of their respective duties, each is a health information custodian within the meaning of *PHIPA*.[6] The relevant sections of *PHIPA* are paragraphs 4.i and 1, respectively, of section 3(1) of *PHIPA*. These sections state:

> "health information custodian", subject to subsections (3) to (11), means a person or organization described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph, if any:
>
> 1. A health care practitioner or a person who operates a group practice of health care practitioners.
>
> 4. A person who operates one of the following facilities, programs or services:
>
> i. A hospital within the meaning of the *Public Hospitals Act*, a private hospital within the meaning of the *Private Hospitals Act*, a psychiatric facility within the meaning of the *Mental Health Act* or an independent health facility within the meaning of the *Independent Health Facilities Act*.

[46] The terms "health care practitioner" and "health care" are further defined in section 2 of *PHIPA*.

[47] "Agent" is also a defined term in section 2 of *PHIPA.* In relation to a health information custodian, an agent is:

> ... a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the

[6] However, as discussed in more detail below, the physicians are not health information custodians when they are acting as agents of THP: section 3(3).

> purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated[.]

[48] THP agrees that it is the health information custodian in respect of the personal health information in its EMR. THP acknowledges that it owns the EMR and controls user access to the EMR, and that its responsibilities include monitoring and auditing access in the EMR, responding to requests for access or correction to information in the EMR, and investigating potential inappropriate accesses in the EMR. In PHIPA Decision 62, the adjudicator took into account similar indicators of ownership and responsibility in determining which party had custody or control of the personal health information in a shared EMR system. In this case, I have no trouble finding that THP has custody or control of the personal health information in the EMR that it owns and manages, and is therefore a health information custodian in relation to that information.[7]

[49] There is some dispute among the parties about the roles of the private practice physicians and their employees when they access THP's EMR for the purposes of providing care to a patient of a private practice that is unrelated to THP. THP asserts that in this role, the physicians are acting as independent health information custodians and not as agents of THP, and that the employees of those physicians are agents of those physicians and not agents of THP.

[50] THP contrasts this situation with what it describes as the more common scenario in which THP employees or credentialed physicians access THP's EMR for the purpose of providing care to THP patients on THP's behalf. In this latter case, THP says, the users accessing THP's EMR are agents of THP, because they are accessing the personal health information in the EMR on behalf of THP, and not for their own purposes. When Physician A or Physician B is providing care to THP patients in this context, and not in the context of his own private practice, the physician is an agent of THP. However, the EMR transactions under review were made in the context of the physicians' private practices, when the physicians were acting as health information custodians independent of THP, and not as agents of THP.

[51] Physician A and Physician B acknowledge that they are health information custodians in respect of their own private practices, and that they therefore have responsibilities under *PHIPA* to ensure the security of any records of personal health information maintained in their own private practice offices, such as their own hard copy patient files. However, they take the position that when they (or their employees) access the electronic portal owned and controlled by THP to view personal health

---

[7] There is no claim that THP is also a "health information network provider" as defined in the regulation to *PHIPA* [General, O Reg 329/04, section 6(2)], and I make no finding in this regard.

information in THP's EMR for the purpose of providing care to their private practice patients, they are *not* independent health information custodians in relation to that information. Among other reasons, the physicians state that their use of the EMR in that transaction is limited to the permissions granted to them by THP, and that they cannot exert any control over the EMR. They note, for example, that they cannot add new patient information to the EMR when they view this information from their private practice offices.

[52] Because the physicians' activities in the EMR in this context are limited in this way, and because the EMR system is owned and controlled by THP, the physicians say that it would not make sense to deem them health information custodians in this transaction, because to do so would permit the "true health information custodian" THP to avoid its responsibilities under *PHIPA* to ensure the security of its EMR. The physicians do not explicitly claim that when they are providing care to their private practice patients, they are acting as agents of THP. However, the physicians appear to argue that when they merely view EMR information (and do not take other steps, such as making a copy of the information for their own private practice files), they should not be subject to the responsibilities of a health information custodian in relation to that information.

[53] I do not agree. I find, instead, that while THP is the health information custodian with custody or control of the personal health information in its EMR, Physician A and Physician B are also health information custodians when they access patient information in THP's EMR for the purpose of providing health care to their private practice patients. Specifically, in the terminology of *PHIPA*, in this transaction, THP is the health information custodian that "discloses"[8] personal health information, and Physician A or Physician B is the health information custodian who "collects"[9] this information from THP, for the purpose of providing health care to a common patient.[10]

---

[8] 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[.]"

[9] 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[.]"

[10] By contrast, when Physician A or Physician B views patient personal health information in THP's EMR as an agent of THP, his viewing is a "use" (and not a collection) of that information: section 6(1) of *PHIPA*. The term "use" is defined at section 2 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."

[54] It is irrelevant that this transaction occurs electronically through an EMR portal, or that the physicians' permissions in the EMR are limited by THP to merely looking at (and does not, for example, allow them to add information to) records of personal health information. Here, I find helpful the analogy drawn by THP between the sharing of patient information between health information custodians through an EMR system and the same exchange done through the perhaps more common method of faxing paper copies of a health record. In each case, regardless of the method of transfer, one health information custodian is disclosing personal health information in his custody or control to another health information custodian, who collects that information, often for the purpose of providing health care to a common patient.

[55] I do not believe that Physician A or Physician B would argue that a hard copy delivery would not qualify as a collection of personal health information by a health information custodian because the collecting custodian cannot alter, add to or otherwise exert control over the disclosing custodian's original records. I also reject the physicians' argument that merely looking at patient information in the EMR (without printing or otherwise retaining a copy of the information in the physician's own record-holdings) means that there has been no "collection" of that information within the meaning of *PHIPA*. There is nothing in the definition of that term in *PHIPA* that would limit it in the manner suggested by the physicians.[11]

[56] Once this disclosure and collection has occurred, the personal health information is also in the custody or control of the collecting custodian. A consequence of this finding is that the collecting custodian, too, has responsibilities under *PHIPA* to ensure that the personal health information that he has collected (or that was collected on his behalf) is handled in accordance with the requirements of *PHIPA*.

[57] I reject the physicians' implicit claim that they do not bear such responsibilities in relation to personal health information that they do not copy or otherwise possess in their own record-holdings. It would not advance *PHIPA*'s purposes to allow a person to

---

(This is the amended version of the definition. While the definition was amended after the date of the breaches at issue, the amendments introduced no substantive changes and do not affect the issues under review.)

I recognize that this definition of use includes "to view" personal health information. In their representations, the parties frequently use the terms "accesses" or "views" to describe the EMR transactions under review. In this decision, I adopt the parties' colloquial use of these terms except where I specifically indicate that I am relying on the meanings given to these terms in *PHIPA*. See also footnote 1.

[11] My analysis is consistent with Part V.1 of *PHIPA*, which, when proclaimed, will set out the framework for a provincial electronic health record (EHR) system. Among other things, this part of *PHIPA* defines certain transactions in the provincial EHR as collections, uses or disclosures of personal health information.

This analysis is also consistent with the IPC's approach to transactions occurring in a shared electronic patient information system. See, for example, PHIPA Decision 102, at paragraph 37.

avoid the responsibilities of a health information custodian simply by choosing not to make a copy of the personal health information that he has collected. Such an interpretation would mean, for example, that none of *PHIPA*'s rules governing uses and further disclosures of personal health information would apply to patient information that the physicians' employees collected by viewing through the EMR portal.

[58] This office's broad and liberal approach to the interpretation of the concept of custody or control in public sector access and privacy legislation is instructive.[12] This approach recognizes that physical possession of a record is not determinative of the question of custody or control, and that relevant factors include the purposes and uses of the record, the extent to which the record is relied upon by an institution, and whether the institution could reasonably expect to obtain a copy upon request.[13] I note, moreover, that the definition of "health information custodian" in *PHIPA* refers to a custodian's having custody or control of "personal health information," rather than of a "record" of that information. In my view, this is further support for my finding that the physicians have custody or control of the personal health information collected through the EMR, regardless of whether they have made their own copies of the information.[14]

[59] Finally, I also find that when an employee of Physician A or Physician B accesses THP's EMR on behalf of the employer physician, in order to assist the physician in the provision of health care to his private practice patients, the employee is acting as an agent of that physician within the meaning of *PHIPA*. I specifically reject the physicians' argument that in this scenario, the employees are acting as agents of THP because it is THP (and not the physicians themselves) who granted the employees the necessary system credentials to access THP's EMR system. In this transaction, as above, THP is the health information custodian that "discloses" personal health information, and the employee is an agent who "collects" this information from THP's EMR on behalf of another health information custodian (namely, the employer physician).

[60] Finding that the respondent physicians are also health information custodians in

---

[12] A number of IPC orders and court decisions have interpreted the phrase "a record in the custody or under the control of an institution" appearing in the *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, at section 10(1); and in the *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56, at section 4(1). See, for example, Order MO-1251 and *Ontario Criminal Code Review Board v. Hale,* 1999 CanLII 3805 (ON CA).

[13] Also see the Supreme Court of Canada's two-part test on the question of whether an institution has control of records that are not in its physical possession: *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25 (CanLII).

[14] The definition of "personal health information" in section 4 of *PHIPA* includes certain information whether it is in oral or recorded form. This also supports my conclusion that it is unnecessary for the custodian to have made his own copy of information in order for *PHIPA*'s rules concerning collection, use and disclosure to apply. See also the discussion of custody or control in *PHIPA* in Halyna Perun et al., *Guide to the Ontario Personal Health Information Protection Act* (Toronto: Irwin Law, 2005) at pages 52-53.

these transactions does not detract from THP's responsibilities under *PHIPA* to protect the personal health information in its EMR, including against unauthorized disclosure. However, as health information custodians in their own right, the physicians also have responsibilities under *PHIPA* when they collect information from THP's EMR, including when they do so through their agents. For example, they must not collect more personal health information than is reasonably necessary for the purpose of the collection, and must take reasonable steps to ensure that the information collected is not used or disclosed for purposes contrary to *PHIPA*. Particularly relevant in these reviews is the duty of health information custodians to take reasonable steps to ensure that their agents act in accordance with *PHIPA* in handling personal health information on their behalf.

[61] The result of these findings is that all the parties involved in a collection and disclosure of personal health information in THP's EMR have responsibilities under *PHIPA* to protect that information. In order to do so, it is essential that all the parties know and understand their respective roles and responsibilities under *PHIPA*. Under the next heading, I will consider these responsibilities in more detail.

Duty to protect personal health information

THP has a duty to take reasonable steps to protect personal health information in the EMR from unauthorized disclosure

The physicians are responsible for personal health information collected without authority by their agents

[62] *PHIPA* requires health information custodians to protect personal health information in their custody or control, including against unauthorized 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.

[63] 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.[15]

[64] A related obligation is the duty for health information custodians to have in place

---

[15] PHIPA Decision 44, at para 140. See also PHIPA Decisions 69, 70, 74, and 80.

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)].

[65] *PHIPA* also addresses the relationship between health information custodians and their agents, including their respective responsibilities with respect to personal health information. Among other things, health information custodians must take steps to ensure that their agents are aware of and understand their obligations under *PHIPA* and under the custodian's information practices. Agents of health information custodians may only collect, use, disclose, retain or dispose of personal health information in accordance with *PHIPA. PHIPA* also makes clear that a health information custodian remains responsible for any personal health information handled on its behalf by its agents.[16]

[66] In the EMR transactions under review, THP, Physician A and Physician B are all health information custodians and must comply with the requirements in sections 10 and 12 to take certain steps to protect personal health information in their custody or control. Additionally, Physicians A and B must ensure that their private practice employees, as agents acting on their behalf in these transactions, are aware of and comply with *PHIPA* and the physicians' information practices, among other duties.[17]

[67] I will next consider whether the collections and disclosures at issue in these reviews were made in accordance with *PHIPA*.

Some of the collections and disclosures at issue were made in contravention of PHIPA

[68] The parties agree that some of the EMR transactions at issue in these reviews were made in contravention of *PHIPA*. Specifically, THP takes the position that accesses made by Employee A or Employee B (or another individual, using that employee's user IDs and passwords) for non–health care purposes are breaches of patient privacy. At the same time, THP appears to take the position that accesses made with the consent of the patient to whom the information belongs may not be privacy breaches, even where there is no apparent health care purpose for the access.

[69] Physician A and Physician B appear to support THP's position.

---

[16] Sections 12(1), 15(3)(b), and 17. While section 17 has been amended since the incidents giving rise to the reviews, the amendments did not significantly alter the responsibilities of health information custodians and agents under *PHIPA.*

[17] *PHIPA* also requires health information custodians that use electronic means to collect, use, modify, disclose, retain or dispose of personal health information to comply with prescribed requirements [section 10(3)]. No such requirements have been prescribed to date.

[70] Above, I found that the EMR transactions at issue in these reviews are disclosures of personal health information from THP's EMR by THP, as well as collections of that same information by agents on behalf of Physician A or Physician B.

[71] I find that while some of these collections and disclosures were made for health care purposes on the basis of assumed implied consent, and were authorized to be made under *PHIPA*, other collections and disclosures were made in contravention of *PHIPA*.

[72] It is irrelevant to this analysis that THP may have had no intention to provide to the physicians' agents any personal health information that the agents were not authorized under *PHIPA* to collect. The definition of "disclose" in *PHIPA* merely requires that THP make available or release personal health information in its custody or control, which THP did by giving the physicians and their agents permissions to access its EMR.[18]

[73] When collecting, using or disclosing personal health information, a health information custodian must comply with section 29 of *PHIPA*. This section states:

> A health information custodian shall not collect, use or disclose personal health information about an individual unless,
>
> a. it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or
>
> b. the collection, use or disclosure, as the case may be, is permitted or required by this Act.

[74] There is no claim that any of the collections and disclosures at issue in these reviews were permitted or required by *PHIPA* to be made without consent.

[75] I agree with THP that some of the collections and disclosures under review were made in compliance with *PHIPA*. In particular, I find that when Employee A or Employee B collected personal health information from THP's EMR for the purpose of assisting in the provision of health care to a private practice patient of Physician A or Physician B, as the case may be, the disclosure by THP (and the corresponding collection by the physician's agent) was made on the basis of the assumed implied consent of the patient [section 20(2)]. This means that where certain conditions are met, the patient's implied consent to the collection, use or disclosure of his or her

---

[18] For a similar analysis, see PHIPA Decision 49, particularly at paragraphs 41-42.

personal health information for health care purposes may be assumed.[19] There is no indication that any of the restrictions that would preclude reliance on assumed implied consent were present in the circumstances. I conclude that these particular EMR transactions were authorized collections and disclosures under section 29(a) of *PHIPA*.

[76] However, for reasons set out below, I do not agree with THP that all EMR accesses made for the purpose of providing or assisting in the provision of health care comply with *PHIPA*. Specifically, I do not agree that accesses made by Employee A or Employee B (or under that employee's user IDs and passwords) to the personal health information of patients of physicians other than Physician A or Physician B comply with *PHIPA*, even if they were made for health care purposes.

[77] THP explained that these transactions may have occurred because Employee A or Employee B shared her unique EMR user IDs and passwords with agents of other private practice physicians who are located in the same medical building as Physician A and Physician B. Or Employee A or Employee B may have done work for another THP-credentialed physician in the same building without having been registered with THP as an EMR user on behalf of that other physician.

[78] THP describes this practice as "credential-sharing," and reports having learned through these investigations that it may have been a widespread practice among agents of the various THP-credentialed physicians with private practice offices in the same medical building. THP acknowledges that this practice contravenes its information practices, because, among other things, credential-sharing could allow unauthorized users to have undetected access to THP's EMR. (Later in this decision, I will discuss the measures taken by THP, and the physicians, to address this issue.) However, THP also appears to suggest that when credential-sharing is done for a health care purpose, then the collection and disclosure of personal health information complies with *PHIPA*. I disagree. Among other reasons, this contravention of the health information custodian's own information practices is itself a contravention of *PHIPA* [section 10(2)].

[79] I also find contrary to *PHIPA* Employee A's and Employee B's accesses to the personal health information of their family members and acquaintances, where those accesses were made for purposes unrelated to the provision of health care to those individuals as private practice patients of Physician A or Physician B, as applicable. This includes any accesses that Employee A made with the consent of the individuals to whom the information belongs. Even assuming without deciding that such collections were "necessary for a lawful purpose" within the meaning of section 29(a) of *PHIPA*, I find again here that such collections made in contravention of THP's (and the physician's) own information practices were made in contravention of *PHIPA*.

---

[19] For a detailed discussion of the requirements of consent, including assumed implied consent, see PHIPA Decision 35.

[80] Having found that many of the collections and disclosures under review were made in contravention of *PHIPA*, I next consider the circumstances that may have contributed to these breaches, and the steps taken by THP and the physicians to address them.

There were deficiencies in THP's and the physicians' policies and practices at the time of these unauthorized collections and disclosures

THP and the physicians have since taken reasonable steps to address these deficiencies

[81] During the IPC's investigation and review, the respondents were asked to describe the administrative, technical and physical safeguards and practices that were in place at the time of the EMR transactions at issue, and any changes to those practices since that time.

The physicians' privacy policies and practices

[82] Physician A admits that during the time of Employee A's employment, Physician A did not conduct formal privacy training with his private practice employees, although he states that he did on several occasions discuss the concept of confidentiality with them. After discovery of the breaches, Physician A made a number of changes to his office's privacy policies and procedures. These include a new requirement that all employees sign confidentiality agreements and attend regular staff meetings that include refreshers on privacy and confidentiality. Physician A also prohibited all but one of his private practice employees from accessing THP's EMR for any reason. The sole employee with access to the EMR only does so in order to view physician's orders and book medical appointments. Physician A also notes that he dismissed Employee A as a consequence of the privacy breaches, and that his remaining employees are aware that termination of employment can be a consequence of a violation of *PHIPA* or his office policies and practices.

[83] Physician B also did not conduct formal privacy training with his private practice employees or require them to sign confidentiality agreements before these breaches came to light. Physician B reports that he now requires his office employees to sign confidentiality and non-disclosure agreements as a condition of employment. These agreements include statements that employees shall not access any patient information except for authorized purposes. Physician B also reports that he has instituted employee training that includes materials prepared by the Ontario Hospital Association, the Ontario Medical Association and the IPC. Since these incidents, Physician B has removed user permissions for any of his private practice employees to access THP's EMR. He has also educated his employees against sharing their log-in credentials for accessing the private practice's own office computers. Physician B notes that he immediately dismissed Employee B upon confirmation of the privacy breaches.

THP's privacy policies and practices

[84] THP provided detailed information about relevant privacy policies and practices in place at the time of the breach incidents, and updates to those policies and practices since that time. These materials include copies of THP policies (including its "Privacy Policy," "Professional Staff and Office Staff Clinical Medical Information Technology Policy" and "Privacy Breach Protocol"), training materials, and documentation requirements for credentialed physicians requesting access to THP's information system (including the EMR) for their private practice employees. Below, I summarize some of this information that is relevant to these reviews.

Privacy policies, practices, education and training

[85] THP explains that it provides different kinds of privacy education and training to different users of its EMR. THP distinguishes between THP staff (for example, hospital employees and professional staff, including THP-credentialed physicians), and non-THP staff (namely, private practice employees of professional staff).

[86] THP explains that at the time of the breach incidents, THP hospital employees (such as nursing and allied health staff) received initial privacy training in person, and annual training through an online module.

[87] In order to become credentialed (i.e., in order to have privileges at a THP hospital), professional staff (including doctors, dentists and midwives) were required to sign confidentiality and privacy agreements stating that they have read and agree to abide by THP policies, including its privacy policy and information technology policy. Credentialed professional staff also completed privacy training on the initial receipt of privileges, and privacy refresher training through a paper-based module during the annual re- credentialing process.

[88] THP explains that the only users of THP's EMR who did not receive privacy training from THP are the employees of private practice professionals. THP takes the position that each private practice professional is responsible for hiring, overseeing and training his or her own employees, who are agents of the private practice professional and not of THP. THP notes that it assists in this process by referring private practice professionals to publicly available privacy training resources (such as the IPC's website, and the websites of the regulatory colleges).

[89] At the time Employee A and Employee B began working for Physician A and Physician B, THP's practice was to grant EMR access to private practice employees of professional staff upon written application by the responsible professional staff. THP explains that based on its agreements with professional staff and its other privacy practices and policies, THP expected that professional staff would comply with *PHIPA* and ensure their employees' compliance with *PHIPA*, including by ensuring that their employees only accessed the EMR when authorized to do so.

[90] THP has since updated its EMR user application process for private practice physicians seeking EMR access for their employees. As of January 2017, private practice physicians and their employees now sign updated application forms that state, among other things, that the employees have read and agree to abide by THP policies, and that the physicians are responsible for any EMR transactions associated with their employees' passwords. All parties are also required to acknowledge and accept that THP provides EMR access to private practice physicians and their employees on the basis that these users will access only personal health information of patients under their care, for purposes authorized by *PHIPA*. All users must also agree not to share their EMR user credentials with any other individuals, and acknowledge that they understand that THP has the right to remove user access for any user who breaches THP's policies or *PHIPA*.

[91] The updated application form also clarifies the nature of the relationship between THP and the private practice physicians. It states, in particular, that the private practice physician operates as an independent health information custodian under *PHIPA* that is separate and distinct from THP, and that, accordingly, the physician is responsible for ensuring *PHIPA* compliance within his own private practice. This includes ensuring that the physician's own private practice employees receive privacy training, with refresher training recommended on an annual basis. In addition, the form specifies that in circumstances where THP decides to notify THP patients of an actual or potential privacy breach originating in the physician's private practice office, the physician's private practice or the particular private practice employee may be named as being responsible for the breach.

[92] THP reports that it intends to further modify the EMR user application process in order to clearly communicate that any access granted to a private practice employee is solely for the purpose of assisting in the provision of care by the named private practice physician for whom the employee works. Where an employee works for more than one private practice physician (as appears to have been the case in these reviews), each private practice physician must sign a separate agreement with THP and agree to comply with the above requirements.

[93] To re-educate existing professional staff with private practice offices of their privacy protection obligations, THP wrote to all these professionals beginning in October 2016. In these letters, THP reminded professional staff of their obligations under *PHIPA*, including the obligation to train and oversee their own private practice employees to ensure *PHIPA* compliance within their private practices. All professional staff were required to provide written confirmation of their understanding of these obligations, failing which the private practice's access to THP's EMR would be cancelled. THP reports that it received responses from 1,114 of 1,282 private practice professional staff, and that it cancelled EMR access for those who did not respond. THP will also begin a process of regular verification of private practice staff credentials, which will require professional staff to confirm, every two years, that their employees continue to require access to THP's EMR. THP notes that this verification is in addition to the

existing requirement (in THP's policies and agreements with professional staff) to promptly notify THP of any staffing changes in the private practice.

[94] In February 2018, new terms were added to the professional staff credential re-application agreement to incorporate the language in the updated EMR user application forms for credentialed physicians with their own private practices. Among other things, the new agreements require that professional staff abide by THP's privacy practices, obtain confidentiality agreements from their private practice employees on an annual basis, provide privacy training to their employees, and implement safeguards to protect personal health information in their own private practices. Professional staff are also required to agree to participate in any privacy investigations arising from the actions of a private practice employee.

[95] Many of these new requirements are reflected in current versions of THP policies. This includes THP's "Professional Staff and Office Staff Clinical Medical Information Technology Policy," which provides that professional staff are responsible for instructing and supervising their office employees in the proper use of THP's information system, and THP's updated "Password Policy," which specifies that computer users must not share their passwords with anyone.

[96] THP also updated other aspects of its privacy training and education for professional staff more generally. This includes an update to the training provided to professional staff on initial credentialing (and annual re-credentialing) to better emphasize THP's privacy policies and expectations for professional staff. To address the particular situations that gave rise to these reviews, THP also provided separate privacy refresher training to Physician A and Physician B in June 2016.

EMR system security

[97] At the IPC's request, THP provided detailed information about its information system and EMR, including about the method of access and use of the EMR, the system's authentication and authorization controls for on-site and remote EMR access, EMR audit processes and capabilities, and THP's methods for detecting unauthorized accesses in the EMR.

[98] The unauthorized collections and disclosures at issue in these reviews were made by individuals who were granted permission to access THP's EMR in their roles as private practice employees of THP-credentialed physicians, in accordance with THP's policy for granting such access. (Or else these transactions were made by other individuals under these employees' user credentials—I addressed above some changes implemented by the respondents to address this practice.) In my view, the unauthorized transactions at issue have less to do with the robustness of THP's EMR system security controls than with the adequacy of the respondents' privacy policies and practices in place at the time of the incidents under review. For example, although THP provided information about its two-factor authentication process for remotely accessing THP's network, and about the EMR user experience, there is no evidence to

suggest that the unauthorized transactions at issue occurred as a result of defects in the network's process for identifying and authenticating users,[20] or in how the EMR's user interface displays information. Given this, I will only briefly address under this heading certain aspects of THP's EMR system security that are relevant in the circumstances of these reviews.[21]

[99] One relevant area is the EMR's audit process and capabilities. THP states that the EMR logs all accesses to the system module that contains the EMR, and produces various types of audit reports. These include reports by patient name, EMR user or device, and reports to detect access to records of patients flagged as confidential or those who have directed that access to their records be restricted (by implementing a "lockbox"). THP also conducts regular random user audits. I note that the unauthorized EMR transactions giving rise to File HR16-131 were detected through one of these random audits. The IPC has recognized the particular importance of audits as a technical safeguard for protecting personal health information held in electronic information systems. Among other benefits, regular audits based on analyzable data about the full extent to which users collect, use, disclose, copy, modify or dispose of personal health information in an electronic system can help to deter and to detect unauthorized activity that contravenes *PHIPA*.[22]

[100] During the course of these reviews, THP revisited its position on the use of privacy flags and warnings in the EMR. At the time of the breach incidents, the EMR displayed privacy flags or warning screens only if a patient had been flagged as confidential, or if the patient's records had been subject to a consent directive or lockbox. THP explained that at the time of the breach incidents, it had not programmed its EMR to display a general privacy warning message because it had had concerns about "alarm fatigue" on the part of EMR users, and because THP believed that its existing privacy training was sufficient to remind users of the need for proper authorization before accessing patient records. Since these incidents, THP has implemented a new privacy warning that appears on the EMR log-in screen, and that is seen by (and must be accepted by) all EMR users each time they log into THP's EMR. The IPC has recognized that privacy notices and privacy warning flags reminding custodians and their agents of their obligations under *PHIPA* and the custodian's privacy policies and procedures may help to prevent or to reduce the risk of unauthorized

---

[20] For example, there is no evidence before me to suggest that the two-factor authentication process could have prevented unauthorized accesses that occurred as a result of an authorized employee's snooping in her family member's medical records, or as a result of the employee's voluntarily providing her authentication factors to another individual.

[21] Other IPC orders and decisions contain extensive discussion of recommended technical and other safeguards specific to EMR and other electronic information systems. These include Orders HO-002 and HO-010, and PHIPA Decisions 64 and 102.

[22] Order HO-013.

access.[23]

[101] Finally, THP provided an update on a project to explore the feasibility of role-based access to the information system housing its EMR. In October 2017, THP completed a role-based access project, based on the principle of least privilege, in which its system users are granted permissions to access different system modules based on their particular roles and the particular categories of personal health information required for each role. The new model of role-based access replaced THP's old method of provisioning new user accounts by "copying-from" an existing user's level of access (where the existing user occupied the same role as the new user). THP explains that, on occasion, using the "copy-from" method of provisioning new user accounts resulted in new users' having greater levels of access than they required (where, for example, the access was "copied- from" an existing user with elevated privileges, despite being in the same role as the new user). The new role-based system of EMR access described by THP would appear to better align with the data minimization principle in *PHIPA*, which provides that no more personal health information should be collected, used or disclosed than is reasonably necessary for the purpose of the collection, use or disclosure [section 30(2)]. An access management strategy that restricts access to personal heath information on a need-to-know basis will also help to minimize the risk of unauthorized access.[24]

[102] I have considered all the evidence from the respondents about the privacy and security measures that each had in place at the time of the breach incidents under review, and the changes that have been implemented since then. It is apparent that there were a number of gaps in the respondents' information practices in place at the time of the breaches.

[103] Several of these stem from the physicians' failure to understand that they are independent health information custodians in respect of the personal health information that they (or their agents) collect from THP's EMR in the context of their private practices. However, this decision (and explicit statements in THP's updated application and credentialing processes, which I will revisit below) now clarify for all parties the roles and responsibilities of THP, the physicians and the physicians' employees in respect of personal health information disclosed by THP and collected by or on behalf of the physicians in the context of their private practices.

[104] The physicians have also taken measures to address gaps in their information

---

[23] Among others, see Orders HO-002, HO-010, and HO-013, and PHIPA Decisions 74 and 102. See also Information and Privacy Commissioner of Ontario, *Detecting and Deterring Unauthorized Access to Personal Health Information* (January 2015), at pages 15-16. Available online: https://www.ipc.on.ca/wp-content/uploads/Resources/Detect_Deter.pdf.

[24] IPC, *Detecting and Deterring Unauthorized Access to Personal Health Information*, cited above, at pages 17-19.

practices that may have enabled their agents' unauthorized activities in the EMR. These include privacy training and education for their private practice employees, and the implementation of confidentiality agreements as a condition of employment. (These practices are also reinforced through the physicians' updated agreements with THP, which now require the physicians to regularly confirm their commitment to ensuring their agents' compliance with *PHIPA* and THP's policies and practices.) It would be prudent for the physicians to require that the privacy training and signing of confidentiality agreements recur on an annual basis, and to ensure that these materials contain plain- language explanations (with examples) of what types of activities are and are not authorized under *PHIPA*. This office has recognized that regular and comprehensive privacy education and training of agents, and the use of confidentiality agreements (that are re-signed on a regular basis) are important tools to help reduce the risk of unauthorized access to personal health information, and to foster a culture of privacy within an organization.[25]

[105] Since the discovery of these breaches, each physician has also introduced limitations on (or has altogether prohibited) their private practice employees' access to THP's EMR, as a further means of preventing or reducing the risk of unauthorized collection of personal health information by their agents. Given the circumstances in which the breaches occurred, the physicians should also expressly prohibit credential-sharing among their agents, both in the context of EMR access (in the event the physicians decide to re-apply for employee access to THP's EMR) and in the context of the physicians' own information systems. The physicians must also take reasonable steps to ensure that their own information systems used to connect to THP's EMR (for example, their computers and network components) are adequately secure to protect the personal health information in it. Finally, the physicians should ensure that all their information practices are set out in writing, and are available to their employees as well as to members of the public (sections 15(3)(b) and 16).

[106] Altogether, considering all the circumstances, I am satisfied that the physicians have taken adequate steps to meet their obligations under *PHIPA*, including the obligation to ensure that any collections, uses and disclosures of personal health information made by their agents on their behalf are made in compliance with *PHIPA.*

[107] Similarly, I find that gaps in THP's information practices in place at the time of the breaches have been adequately addressed by THP through changes it has implemented to its policies and practices, particularly those addressing professional staff who operate private practices.

---

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

[108] I agree with THP that it is not THP but rather the private practice professionals who bear direct responsibility for the private practice employees' handling of personal health information. At the same time, THP recognizes that there is overlap in the responsibilities of THP and private practice professionals to protect the information that agents of the private practice collect, and that THP correspondingly discloses, from THP's EMR. In addition to clearly identifying that professional staff are health information custodians in respect of their own private practices (and are thus responsible for ensuring their agents' compliance with *PHIPA*), THP has taken the further precautions described above to ensure that private practice employees given access to THP's EMR are adequately trained and supervised by their employers. These include the new requirements that private practice professionals confirm to THP their commitment to providing periodic privacy training to their employees, and that all EMR users (including the employees) affirm their understanding of THP policies as a condition of being granted EMR access. I find these to be reasonable measures by THP to mitigate the risk of unauthorized activity in its EMR by private practice employees. I also suggest that, where it has not already done so, THP clearly identify in its agreements and policies that such employees are "agents" within the meaning of *PHIPA* of the private practice professionals, and not of THP.

[109] THP has also taken steps to re-educate its own staff (hospital employees, as well as professional staff) of their obligations when handling personal health information in THP's EMR, whether or not it is done on THP's behalf. These include directed refresher training for the two physicians involved in these incidents, as well as more general updates to THP policies and the privacy training given to THP staff (including professional staff). Notably, these changes include an explicit instruction that information system users not share their user IDs and passwords. This prohibition is meant to address the problem of credential-sharing that appears to have been a widespread practice among remote access users of THP's EMR, and a source of some of the unauthorized transactions at issue in these reviews. I also observe that although this decision is not directed at the number of other THP-credentialed professional staff who operate their own private practices (including those with practices in the same medical building as Physician A and Physician B), the measures implemented by THP will equally apply to them. Taken together, I am satisfied that through its policies, agreements and practices governing access to and oversight of activity in its EMR, THP has put into place reasonable measures to protect the security of EMR information.

[110] Overall, I am satisfied that THP has taken adequate steps to identify and to address gaps in its information practices that may have enabled the breaches that gave rise to these reviews, and that these improved practices, along with its ongoing practices (like its regular program of monitoring and auditing accesses in the EMR) will help it to comply with its obligations under *PHIPA*. All the respondents should be

mindful of the need to revisit their information practices on a regular basis.[26] The IPC has noted that privacy practices and safeguards that are reasonable at one time may no longer be reasonable with the passage of time, development of new technologies, and identification of new risks.[27]

[111] Finally, I am also satisfied that the respondents THP and the physicians responded adequately to the privacy breaches, including by cooperating with the IPC's investigations and reviews into these matters. The chronology of events following discovery of the breaches, described in detail earlier in this decision, demonstrates diligent and effective efforts by the respondents to contain, remediate and investigate the breaches. I conclude that the respondents complied in this respect with their obligations under section 12(1) of *PHIPA*.

THP provided notice to some affected patients in accordance with PHIPA

THP can satisfy its notice obligations to some other affected patients through alternative means

[112] Lastly, I asked THP and the physicians whether notice had been given to affected individuals in accordance with section 12(2) of *PHIPA*. The version of section 12(2) that was in effect at the time of the breaches under review stated:

> Subject to [a subsection of *PHIPA* that does not apply in the circumstances of this review] and subject to the exceptions and additional requirements, if any, that are prescribed, a health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.[28]

[113] In particular, I asked THP and the physicians to identify the health information custodian responsible under section 12(2) to notify affected individuals whose personal health information was handled without authority in THP's EMR, and whether all the individuals to whom notice was required to be given under section 12(2) were, in fact, notified. In addition, because a determination about notice in the context of these reviews may have an impact on other hospitals that maintain and grant user access to

---

[26] Among others, see Orders HO-004 and HO-010.
[27] Among others, see Orders HO-010 and HO-013, and PHIPA Decisions 64 and 70.
[28] Section 12(2) has been amended since the date of the breaches at issue. Among other things, section 12(2) now explicitly requires that notices include a statement that notified individuals have a right to make a complaint to the IPC. (I note that in any case, some (but not all) of the notification letters sent by THP to affected patients included such a statement.) The amendment also replaced the term "accessed by unauthorized persons" with "used or disclosed without authority." These and other changes introduced by the amendment have no substantive impact on the issues in these reviews.

EMRs, I asked the Ontario Hospital Association (OHA) for its views about which party has responsibility for providing notification under section 12(2) in the case of a breach. The OHA provided representations, which I describe below.

[114] I noted above that through its investigation and the IPC process, THP notified a number of individuals whose personal health information THP determined had been accessed without authority by Employee A or Employee B (or under their user credentials). THP also explained why it had chosen not to notify a significant number of other individuals for whom THP was unable to determine the precise reason for access.

[115] Despite the fact that it had made these decisions about notification, THP initially took the position that it is the obligation of the physicians, and not of THP, to notify patients when physicians' private practice employees access patient personal health information in THP's EMR without authorization.

[116] However, in its later representations to me made during these reviews, THP accepts that it is responsible for notifying patients when its EMR is accessed without authorization. This includes situations (like the ones at hand) where THP improperly discloses and private practice physicians who are independent health information custodians (or agents of those physicians) improperly collect personal health information from THP's EMR.

[117] Physicians A and B appear to support THP's position. Each physician confirmed that he did not independently notify any patients under section 12(2), and instead relied on THP's notification of affected parties. Among other reasons, the physicians note that THP (and not the physicians) conducted the audits and investigations that led to the discovery of the employees' unauthorized EMR transactions, and that the physicians had no reason to believe that THP failed to identify and notify all the parties to whom notice was required to be given under section 12(2). The physicians also note that they are explicitly named in THP's notification letters to affected individuals (in explaining that an employee of the physician was the source of the breach), giving those individuals an opportunity to contact the relevant physician directly. (There is no indication that any of the affected individuals contacted the physicians directly after being notified of the breach by THP.)

[118] The OHA takes a different position. In its view, each private practice physician is the health information custodian responsible for the breach by his agent, and is therefore responsible for notification to the affected patients. In the OHA's submission, to make THP (and, by extension, other hospitals that maintain and grant user access to EMRs) responsible for activity they do not directly control will discourage hospitals from implementing EMR systems, and could ultimately impede efforts to establish a provincial electronic health record system.

[119] In addition, the OHA says, privacy protection is best accomplished by clearly placing the accountability for private practices on the physicians themselves. The OHA asserts that hospitals that maintain and grant access to EMRs cannot reasonably be

expected to assume liability and notification responsibilities for a breach resulting from activity outside their control. The OHA notes that while the private practice employer has the ability to hire, discipline and fire his agents for a breach of the rules, hospitals have no such power or ability to control the essential risks that arise out of the employer's independent activities.

[120] I found, above, that in the EMR transactions under review, both THP and the private practice physicians are independent health information custodians, each with their own duties under *PHIPA* to protect personal health information accessed through THP's EMR. All the parties agree that the physicians alone are responsible for hiring, supervising, monitoring and disciplining their employees.

[121] This does not mean, however, that only the private practice physicians have responsibilities under *PHIPA* in the event of a breach by their agents in relation to THP's EMR. Both THP and the private practice physicians recognized their respective obligations to respond adequately upon discovery of the breaches, including by taking steps to contain and remediate the breaches. As the health information custodian responsible for the security of the EMR, THP immediately suspended the employees' access to the EMR, audited the employees' activities in the EMR, and took steps to improve its EMR security, such as introducing new policies to confirm the identity of specific agent users of its EMR and to prohibit the sharing of EMR user credentials. As the health information custodians responsible for their employees' activity in the EMR, the physicians cooperated with THP's audit investigations to determine the extent of the breaches, revised their office practices for employee access to the EMR, and ultimately dismissed the employees who had collected personal health information in contravention of *PHIPA*.

[122] In the cases under review, THP and the private practice physicians also treated THP as the health information custodian responsible for notifying affected individuals of the private practice employees' unauthorized accesses in THP's EMR. In these circumstances, I agree that THP was the appropriate party to give notice under section 12(2) of *PHIPA*. As the health information custodian who maintains the EMR, THP was best placed to discover and investigate the extent of the employees' activity in the EMR, identify all the parties whose personal health information had been accessed without authority, and initiate contact with these individuals, all of whom are THP patients, but some of whom may not have any relationship with the particular private practice physician for whom the employee worked. In these cases, notification by THP was appropriate, taking into account not only the language of section 12(2)[29] but also the interests of the affected individuals.

---

[29] Neither the previous nor the amended version of section 12(2) imposes an obligation on custodians to notify in the event of an unauthorized collection of personal health information.

[123] I also agree with THP that in some circumstances, notification by the collecting custodian may be more appropriate, and a reasonable approach to fulfilling the notice obligation in section 12(2). For example, in a case where the private practice physician has a more significant relationship with the patient whose privacy was breached, notice from that physician (rather than from the custodian who disclosed the information) may be prudent. So long as the notice is given as required upon the events described in section 12(2) (and complies with the other requirements of that section), I agree with THP that circumstances such as the patient's interests and the relationships between the patients and the various custodians involved may be relevant factors in deciding how best to fulfil the notification obligation. I am not persuaded that applying such an approach to notification in future cases would have the consequences of discouraging hospitals from adopting EMR technologies, or from participating in broader initiatives like a provincial electronic health record system.

[124] Finally, I am generally satisfied with THP's efforts to identify affected individuals for the purposes of notification under section 12(2). However, I also found, above, that some of the EMR transactions investigated by THP were contraventions of *PHIPA*, despite THP's opposite conclusion and its consequent decision not to notify certain individuals. In particular, I found that EMR accesses made by the private practice employees to the records of patients of physicians other than Physician A and Physician B were made in contravention of *PHIPA*. I found that any instances of accesses made by other individuals under those employees' user credentials—through "credential-sharing"—were also contraventions of *PHIPA*. I also found that other accesses made by the employees to the records of their families and friends for non–health care purposes were also contraventions of *PHIPA*.

[125] For these affected individuals, I am satisfied that the notification requirement can be met through a more flexible approach. Among other reasons, I accept THP's evidence that many of these accesses were more likely than not made for health care purposes or with the consent of the individual, and find that these factors diminish the urgency for notice in these circumstances, where many of these unauthorized transactions date back many years or may already be known to the individuals. I also find relevant THP's evidence that despite the large number of notices it did give in both cases (and the number of contacts from previously unidentified parties), as well as the substantial level of media attention surrounding one of these breach incidents, THP has not received any additional complaints or inquiries from the public about improper access by these employees.

[126] In these circumstances, I will not require THP to issue additional individual notices at this stage. Instead, it is reasonable for THP to fulfil its notice obligations through alternate means, such as by including notes in the files of the affected patients. In addition, although I have found that the physicians do not have a legal obligation to notify in these circumstances, I encourage them to post notices in their private practices advising their patients of this decision. All such notified patients should be directed to a contact person at THP who can address any questions they may have

about these incidents, or about accesses to their particular records.

[127] For all the reasons given above, I conclude that deficiencies in the respondents' practices identified through THP's investigations and these reviews have been addressed or will be addressed by the respondents. Overall, I am satisfied with the steps taken by the respondents to respond to the privacy breaches and to implement changes to their information practices to comply with their obligations under *PHIPA*. Although I have made a number of comments and recommendations in this decision, I conclude that it is unnecessary to issue any order in the circumstances.

NO ORDER:

For all the foregoing reasons, I conclude my reviews under section 58(1) without issuing any order.

Original Signed by: February 18, 2020

Jenny Ryu
Adjudicator