Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 298

Complaints HR24-00320, HR24-00321, HR24-00409

Windsor Regional Hospital, Chatham-Kent Hospital Alliance, Erie Shores Healthcare, WE Kidz Pediatrics, and Dr. Omar Afandi

August 27, 2025

Summary: This decision addresses a privacy breach reported under the *Personal Health Information Protection Act, 2004,* by Windsor Regional Hospital (WRH), Chatham-Kent Health Alliance and Eries Shores HealthCare (collectively, the Hospitals). The Hospitals reported to the Information and Privacy Commissioner of Ontario that a physician with privileges at WRH used his access to the Hospitals' shared electronic health record system to conduct targeted searches for newborn males and then contacted the parents to offer them circumcision services through his private pediatric clinic, WE Kidz Pediatrics (WE Kidz).

In this decision, the Commissioner considers whether WRH and WE Kidz took reasonable steps to protect against unauthorized collection, use and disclosure of personal health information within their custody or control; whether WRH and WE Kidz had information practices in place and whether they complied with those information practices; whether WRH and WE Kidz responded adequately to the breach; and, whether administrative monetary penalties should be imposed against the physician and/or WE Kidz.

In this decision, the Commissioner makes no order against the Hospitals but makes a number of recommendations to WRH to improve its record-keeping and information practices to ensure that WRH can more effectively demonstrate compliance with its obligations under *PHIPA*.

The Commissioner determines that AMPs are appropriate in the circumstances and orders an AMP of $5,000 to be imposed against the physician and an AMP of $7,500 against WE Kidz for contraventions under *PHIPA.* She also orders that the physician and WE Kidz securely dispose of

all records containing personal health information inappropriately obtained from the shared EHR system and used by the physician to offer circumcision services at WE Kidz.

Finally, the Commissioner recommends that WE Kidz strengthen its privacy policies and procedures to ensure that it meets its obligations under *PHIPA* and that WE Kidz management and staff undergo further privacy training.

Statutes Considered: *Personal Health Information Protection Act, 2004,* SO 2004 c 3, Sched A, as amended, sections 2(1), 3(1), 4(1), 10, 11.1, 12, 17, 29, 58(1), 61, 61.1; O Reg 329/04: General, section 35.

BACKGROUND:

[1] On May 31, 2024, my office received a breach report on behalf of Windsor Regional Hospital (WRH), Chatham-Kent Health Alliance (CKHA) and Erie Shores HealthCare (ESHC), collectively "the Hospitals".

[2] The case involves Dr. Omar Afandi, a physician with privileges at WRH, who used his access to the electronic health record system shared by the Hospitals to conduct targeted searches for newborn males. He then contacted the parents to offer them circumcision services through 1000812873 Ontario Inc. o/a WE Kidz Pediatrics (WE Kidz), a clinic in Windsor which he partly owns.

[3] Upon receiving the Hospitals' breach report, my office (the Office of the Information and Privacy Commissioner of Ontario, or IPC) opened a file. On October 28, 2024, Dr. Afandi and WE Kidz were added as respondents.

[4] On March 6, 2025, given the seriousness of the allegations, I decided to commence a formal review of this matter under section 58(1) of the *Personal Health Information Protection Act*, *2004* (*PHIPA*, or the *Act*) and, in particular, to decide whether the imposition of administrative penalties (AMPs)[1] under section 61.1 of *PHIPA* is warranted in this case.

[5] I sought and received representations and replies from all parties. Dr. Afandi requested, and I agreed, to keep confidential some of his representations from the Hospitals. I exercised this discretion in accordance with section 18.03(d) of the IPC's *Code of Procedure for Matters under the Personal Health Information Protection Act, 2004*.[2] Dr. Afandi provided these representations to the IPC in confidence and confidentiality was essential to secure the full participation of Dr. Afandi in this process.

---

[1] Section 61.1 of *PHIPA* gives the IPC the discretion to issue administrative penalties as part of its enforcement powers for violations of *PHIPA*. Such administrative penalties or APs are also commonly referred to as administrative monetary penalties or AMPs. In this decision I will refer to the administrative penalties referred to in section 61.1 of *PHIPA* as AMPs.

[2] https://www.ipc.on.ca/en/search?keywords=Code+of+Procedure+PHIPA

[6] Moreover, Dr. Afandi no longer holds privileges at WRH, has accepted responsibility for his actions and has made no allegations against the Hospitals. Sharing this information with the Hospitals when there is no need for them to have it is not necessary for procedural fairness purposes and there is unlikely any benefit to be gained from sharing the information for the disposal of this file.

[7] Where, however, I received the same or similar submissions from other parties or in other submissions of Dr. Afandi that were not subject to a request for confidentiality that was granted by the IPC, I have referred to them as necessary to establish the basis of my decision.

FACTS:

[8] The facts below were either relayed to the IPC through the Hospitals' breach report, gathered during the Early Resolution process or provided by the parties in response to my Notice of Review.

[9] On April 26, 2024, CKHA's Women's & Children's Program received a report from a patient regarding unauthorized use of her personal health information (PHI). The patient had delivered a baby at CKHA the day before and, while still an inpatient at CKHA, received a call from WE Kidz asking if she would be interested in having her newborn circumcised. The patient inquired whether CKHA staff shared patient information with clinics that offer services like circumcision. CKHA staff assured the patient that they did not share any PHI without patient consent, and that patients generally self-refer for services such as circumcision.

[10] The patient called WE Kidz back and asked how they obtained her information. The patient was advised that WE Kidz was a new clinic started by a physician who had access to the CKHA's electronic records where he could look up male newborns and relevant contact information. The patient advised CKHA of this that same day.

[11] Upon being advised of the issue, the CKHA Privacy Office initiated an investigation. It engaged TransForm Shared Services Organization (TSSO), the provider of technology and health care services solutions for the Hospitals. The Hospitals shared a remote-hosted EHR system known as Oracle Health/Cerner (the shared EHR system or the EHR system).

[12] On May 6, 2024, CKHA received a similar report from another CKHA patient. That patient advised that, on May 3, 2024, she received a voicemail from a physician inquiring if she would be interested in circumcision for her newborn. On May 4, 2024, the physician called the patient a second time. The patient asked how the physician received her phone number and information. The physician told the patient that he had access to the Hospitals' shared EHR system and could see patient names and contact information without opening patients' charts. When the patient pressed the caller for more details, the physician ended the call.

[13] CKHA initiated an investigation into this second patient report.

[14] On May 7, 2024, given that the physician who contacted CKHA patients told them he held privileges at WRH, CKHA advised WRH of these concerns.

[15] That same day, WRH's Chief of Staff contacted Dr. Afandi, who confirmed that he had (a) accessed lists of the Hospitals' patients through the shared EHR system (b) searched in the shared EHR for patients based on date of birth and sex, and (c) in certain instances, contacted patients directly by phone to offer circumcision services at WE Kidz. WRH's Chief of Staff directed Dr. Afandi to immediately cease this practice across all hospitals in which he had access to patient information and Dr. Afandi agreed to do so.

[16] WRH and CKHA directed TSSO to confirm the scope of the personal health information that had been inappropriately accessed/used and to verify that no other physician had conducted similar searches.

[17] The TSSO Investigation confirmed that Dr. Afandi used search features within the shared EHR system to collect newborn and mother contact information. Specifically, the investigation found that Dr. Afandi had conducted "person searches" querying the system by sex (i.e., "male") and date of birth, and that he had conducted these searches 146 times through which he was able to access and view the PHI of potentially 831 patients. Dr. Afandi was able to view information such as, patient name, Medical Record Number (MRN), date of birth, sex, encounter-related information, phone number, and health card number. Dr. Afandi did not, however, access individual patient charts.

[18] WRH's Chief of Staff wrote to Dr. Afandi on May 15, 2024 advising that, as a result of his unauthorized collection and use of PHI, he would be immediately removed from the on-call schedule for the remainder of his locum appointment (expiring May 31, 2024) and he would no longer be permitted to exercise his privileges effective that same day. WRH submits that it gave Dr. Afandi the opportunity to withdraw his application for reappointment for the 2024-2025 credentialing year.

[19] On May 16, 2024, Dr. Afandi confirmed through his legal counsel that he was withdrawing his application for reappointment. Effective May 31, 2024, Dr. Afandi no longer holds privileges at WRH.

[20] The Hospitals notified the IPC of this breach on May 31, 2024. On June 1, 2024, WRH also reported Dr. Afandi to the College of Physicians and Surgeons of Ontario (CPSO).

[21] The Hospitals, collectively, sent notification letters to potentially affected individuals via postal mail during the week of July 2, 2024. These notification letters included details of the breach, specifics of the PHI at issue, the steps taken to address the breach, the fact that the IPC was notified of the breach, information on how to file a complaint with the IPC, and a hotline number to call in case of any questions.

[22] The Early Resolution Analyst originally assigned to this file sent a Notice to Dr. Afandi and WE Kidz relaying the allegations in the Hospitals' breach report, along with a series of questions. Both Dr. Afandi and WE Kidz responded on November 15, 2024. Although they provided separate responses, many aspects of their responses were substantially similar and can be summarized as follows.

[23] Dr. Afandi acknowledged that between April 20 and May 7, 2024, he accessed the Hospitals' shared EHR system to search for newborn males for the purpose of contacting their parents to offer circumcision services at WE Kidz.

[24] Dr. Afandi searched through the shared EHR system and when he identified a recently born male infant at CKHA or ESHA, he inserted the associated telephone number into his phone through an application called Weave. He stated that he used Weave to send text messages informing families of his circumcision services performed at WE Kidz. He also stated that he called some patients directly from the WE Kidz telephone number.

[25] Dr. Afandi acknowledged that his accesses were unauthorized under *PHIPA* but submits that he only learned this after speaking with WRH's Chief of Staff on May 7, 2024, and he immediately stopped thereafter.

[26] Dr. Afandi reported that he contacted 17 parents of male infants by text messages. He also advised that his call logs from his extension at WE Kidz show 74 calls to unique telephone numbers made between April 20 and May 7, 2024. Dr. Afandi states that most of these calls were to his own patients but acknowledges that some were likely made to potential circumcision patients who were outside his circle of care. He provided charts setting out all numbers, dates and times of calls, as well as copies of the text messages he sent.

[27] Dr. Afandi informed the IPC that he did not retain any PHI, other than the logs of messages and phone calls he kept for "investigation" purposes, the telephone numbers of the individuals he contacted, and the PHI relating to individuals on whom he performed circumcisions.

[28] Dr. Afandi reported that, of the individuals he contacted, he is aware of one patient from CKHA who booked a circumcision appointment with him due to his phone solicitation. The cost for the circumcision procedure was $350. Dr. Afandi states that $35 of this amount went to WE Kidz as an overhead payment.

[29] Dr. Afandi acknowledged having received Privacy, Security and Confidentiality training on the shared EHR system in October 2020 and January 2021. He also stated that he read WRH's privacy module when he applied for reappointment in April 2024. He acknowledged that he signed a confidentiality agreement when he applied for privileges at WRH in 2020.

[30] All parties to this matter were provided a copy of the above facts in my Notice of Review and given the opportunity to comment on their accuracy or to state their

disagreement with any of them. As no party stated their disagreement, I find the above facts to be true and they form the factual basis for my decision, subject to any additional findings set out below.

SCOPE OF DECISION

[31] In this decision, I have decided to focus on Dr. Afandi's collection, use and disclosure of PHI from the shared EHR system. Although the Hospitals reported other facts to my office as part of their privacy breach report, I have decided not to address them for the following reasons.

[32] The Hospitals reported that, on or around April 29, 2024, WRH was made aware by its own staff that Dr. Afandi had been offering WRH patients circumcision services at WE Kidz. That same day, the Chief of Pediatrics at WRH addressed the concern with Dr. Afandi who acknowledged that during his rounds at WRH, he had offered WE Kidz circumcision services to a WRH patient under his care. The Chief of Pediatrics at WRH stated: "While it is okay for you to accept referrals for the procedure at your practice, soliciting this family to use your services is of concern". He further cautioned Dr. Afandi against this practice and provided him with the CPSO Policy with respect to advertising /contacting /targeting individuals regarding services.

[33] In response to these allegations, Dr. Afandi maintains that he did not solicit circumcision services when rounding at WRH. Dr. Afandi informed the IPC that he was on call at WRH on April 27 to 28 doing rounds on newborns during that time. He indicated that one family asked about circumcisions and that, in response, he explained the different methods of the procedure and stated that he performs circumcisions at his clinic, WE Kidz. Dr. Afandi submitted that this patient was within his circle of care, and that they had already decided to do the circumcision at WRH but the doctor who was originally supposed to do the procedure was late and the family was ready to be discharged. He submitted that the family ultimately decided to have Dr. Afandi perform the circumcision at WE Kidz at a cost of $350. This is a different patient than the one who booked a circumcision with Dr. Afandi pursuant to his phone contact with them using the telephone number he obtained from the shared EHR system (described above).

[34] For the purposes of this decision, I will not be addressing Dr. Afandi's offer of private circumcision services to parents of newborns during rounds at WRH. WRH maintains that use of patients' PHI was not authorized under section 29 of *PHIPA* and that Dr. Afandi should have performed the circumcision procedure at WRH not WE Kidz. It maintains that not doing so was a breach of Dr. Afandi's obligations under the WRH by-law with respect to conflict of interest, and the CPSO Policy: *Conflict of Interest and Industry Relationships.*[3]

[3] https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Physicians-Relationships-with-Industry-Practice.

[35] It appears from the submissions of all parties that Dr. Afandi was the attending physician on duty at WRH at the time this patient asked him about circumcision procedures. It appears, though I do not necessarily find, that the patient in question was in Dr. Afandi's circle of care and he would have had legitimate access to the patient's chart. Moreover, it also appears uncontested that the patient took Dr. Afandi up on his offer to have circumcision services performed at WE Kidz.

[36] In these circumstances, the privacy issue associated with Dr. Afandi's use of this WRH patient's personal health information is secondary to the question of whether his conduct in these circumstances constituted an inappropriate solicitation contrary to his professional obligation under the Hospitals' and the CPSO's conflict of interest policies. That question is currently before the CPSO and is more directly in its remit than mine. For this reason, I have decided to leave determination of this specific solicitation issue to the CPSO.

[37] Also, as regards to the Hospitals, I have decided to focus on WRH. As set out below, WRH is where Dr. Afandi held privileges as a professional staff member and is the Hospital on behalf of whom he was acting as agent at the time of the breach. As such, the training and other safeguards put in place by WRH are of greatest relevance to this matter and are the focus on my below analysis. Of course, this should not be read as diminishing the obligations of the other Hospitals in relation to the PHI in the shared EHR system.

PRELIMINARY FINDINGS

[38] In my Notice of Review sent to all parties on March 6, 2025, I set out several preliminary findings necessary to confirm how the *Act* applies to the above facts and asked whether any of the parties disagreed. None disagreed with these preliminary findings, and therefore, I find the following:

The EHR information accessed by Dr. Afandi in this case, which includes, patient name, medical record number, date of birth, sex, encounter-related information, phone number and health card number, constitutes "**personal health information**" (PHI) within the meaning of section 4(1) of the *Act*;

- WRH, CKHA, ESHC and WE Kidz are "**health information custodians**" (custodians) within the meaning of section 3(1) of *PHIPA*[4];

[4] Under s. 3(1)4i of *PHIPA* (a person who operates a hospital within the meaning of the *Public Hospitals Act*) and s. 3(1)1 of *PHIPA* (a person who operates a group practice of health care practitioners).

- At the time of the reported breaches, Dr. Afandi was an "**agent**" of WRH and WE Kidz as that term is defined in section 2(1) of *PHIPA*;

- The PHI in the shared EHR system at issue was in the **custody or control** of one or more of the Hospitals[5];

- When Dr. Afandi contacted individuals using information from the shared EHR system to offer circumcision services to be performed at WE Kidz, through his phone or the WE Kidz telephone number, the information at issue was PHI in the **custody or control** of WE Kidz;

- Dr. Afandi's actions at issue in this matter constituted **collections, uses** and **disclosures** of PHI within the meaning of section 2(1) of *PHIPA;*

- When Dr. Afandi added patient contact information from the shared EHR system into his smartphone to contact patients to offer circumcision services at WE Kidz, this was a **collection** of PHI by WE Kidz and a **disclosure** of PHI by the hospital with custody or control of the PHI;

- Dr. Afandi's utilization of contact information obtained from the shared EHR system to text or phone individuals to offer them circumcision services at WE Kidz was a **use** of PHI by WE Kidz; and

None of the **collections**, **uses** and **disclosures** of PHI at issue in this matter were authorized under section 29 of the *Act* as they were not done with the consent of the individual and were not necessary for a lawful purpose or otherwise permitted or required by *PHIPA*.

[39] Given no disagreement by any of the parties, I therefore make the above preliminary findings and go on to consider the main issues in this review.

ISSUES:

A. Did WRH and WE Kidz take reasonable steps to protect against unauthorized collection, use and disclosure of PHI within their custody or control?

B. Did the WRH and WE Kidz have information practices in place, and did they comply with those information practices?

C. Did WRH and WE Kidz respond adequately to the privacy breach?

[5] For the purposes of this decision, I do not need to determine which of the Hospitals had custody or control of which PHI accessed by Dr. Afandi in the shared EHR system. This is because, regardless of which Hospital had custody or control, there is no dispute that Dr. Afandi's actions were unauthorized collections, uses or disclosures of PHI under *PHIPA* and that he was acting as agent of WRH at the time.

D. Given the circumstances of this matter, should the IPC impose AMPs or any other order against Dr. Afandi and/or WE Kidz?

DISCUSSION:

Issue A: Did WRH and WE Kidz take reasonable steps to protect against unauthorized collection, use and disclosure of PHI within their custody or control?

[40] Having already established that Dr. Afandi, acting as agent of WRH and of WE Kidz, collected, used and disclosed PHI without authorization, the first issue to determine is whether the Hospitals and WE Kidz, as custodians, took reasonable steps to prevent such unauthorized actions from happening.

[41] Under *PHIPA*, custodians have significant responsibilities to protect PHI within their custody or control, including PHI handled by their agents. Specifically, section 17 of *PHIPA* provides as follows:

> 17 (1) A health information custodian is responsible for personal health information in the custody or control of the health information custodian and may permit the custodian's agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if,
>
> > (a) the custodian is permitted or required to collect, use, disclose, retain or dispose of the information, as the case may be;
> >
> > (b) the collection, use, disclosure, retention or disposal of the information, as the case may be, is necessary in the course of the agent's duties and is not contrary to this Act or another law; and
> >
> > (c) the prescribed requirements, if any, are met.
>
> (1.1) A permission granted to an agent under subsection (1) may be subject to such conditions or restrictions as the health information custodian may impose.
>
> (2) Subject to any exception that may be prescribed, an agent of a health information custodian may collect, use, disclose, retain or dispose of personal health information only if,
>
> > (a) the collection, use, disclosure, retention or disposal of the information, as the case may be,

> (i) is permitted by the custodian in accordance with subsection (1),
>
> (ii) is necessary for the purpose of carrying out his or her duties as agent of the custodian,
>
> (iii) is not contrary to this Act or another law, and
>
> (iv) complies with any conditions or restrictions that the custodian has imposed under subsection (1.1); and
>
> (b) the prescribed requirements, if any, are met.
>
> (3) A health information custodian shall,
>
> (a) take steps that are reasonable in the circumstances to ensure that no agent of the custodian collects, uses, discloses, retains or disposes of personal health information unless it is in accordance with subsection (2); and
>
> (b) remain responsible for any personal health information that is collected, used, disclosed, retained or disposed of by the custodian's agents, regardless of whether or not the collection, use, disclosure, retention or disposal was carried out in accordance with subsection (2).
>
> (4) An agent of a health information custodian shall,
>
> (a) comply with the conditions or restrictions imposed by the health information custodian on the agent's collection, use, disclosure, retention or disposal of personal health information under subsection (1.1); and
>
> (b) notify the custodian at the first reasonable opportunity if personal health information that the agent collected, used, disclosed, retained or disposed of on behalf of the custodian is stolen or lost or if it is used or disclosed without authority.

[42] Further, section 12(1) of the *Act* requires custodians to take "reasonable" steps to protect PHI in their custody or control against unauthorized use or disclosure, among other things.

> 12 (1) 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.

[43] Section 11.1 of the *Act* also requires custodians "to take steps that are reasonable in the circumstances to ensure that personal health information is not collected without authority."

[44] I will assess the reasonableness of each custodian's privacy protection measures against these statutory requirements.

Representations of the Hospitals

[45] The Hospitals stated that at the time of the breach they had the following measures in place:

- With respect to the shared EHR system, the Hospitals had a Regular Member Services Agreement with TSSO (2022) setting out the relationship between the parties, and providing for, among other things, security and audits of the system.
- The Hospitals had a Regional Data Governance and Security Steering Committee, a Regional Data Governance Working Group, and a Regional Data Management Working group to ensure that the Hospitals, among other things:
    - take a consistent approach to ensuring the successful deployment of data governance related tasks and initiatives from a regional and site-specific data management lens;
    - maintain a standardized process for system access to the shared EHR; and
    - align on legal requirements and industry best practices for the protection of PHI on the shared EHR system.
- Each Hospital had implemented and continues to maintain privacy and information security programs designed to protect PHI in their custody or control "consistent with PHIPA and guidance issued by the IPC". Such policies include policies on the collection, use, modification, disclosure, retention and disposal of PHI, as well as privacy breach protocols.
- At the time of the breach, the Hospitals were conducting and continue to conduct random and ad-hoc audits of accesses to PHI on an ongoing basis in accordance with their auditing and monitoring policies.

[46] More specifically, with respect to WRH, where Dr. Afandi held privileges and on behalf of whom he was acting as an agent, WRH stated that it had the following measures

in place at the time of the breach:

- The forms for appointment and reappointment at WRH required every applicant to attest to the following:

- *I have read and hereby provide all of the undertakings and acknowledgements required of all applicants to the Professional Staff as set out in the By-Law.*

- The WRH by-law required every applicant for appointment or reappointment of privileges to confirm (among other things) that they have read the by-law, the Rules and Regulations, the hospital's mission, vision and strategic plan, and its clinical, administrative and human resources policies and procedures, and that they undertake to act in accordance with these as they may be established or revised from time to time.

- The WRH by-law further required applicants for appointment or reappointment to acknowledge that their failure to comply with applicable Legislation, Rules and Regulations, will constitute a breach of their obligations to WRH, and may result in the removal of access to resources and/or restriction, suspension, revocation or denial of their privileges. The by-law defines "Legislation" as including *PHIPA,* and defines "Rules and Regulations" as including WRH policies governing the practice of medical staff both corporately and within a particular department.

- WRH's Privacy Policy required its professional staff to sign a Confidentiality Agreement upon hiring and annually thereafter, acknowledging that they had read, understood and committed to maintaining WRH's confidentiality expectations at all times. Professional staff were also required to sign an Access Acknowledgement, and a Remote Access Agreement which WRH submits contained "robust" privacy and confidentiality obligations.

- WRH required its professional staff to undergo training, at onboarding and annually, in respect of their privacy and security obligations under *PHIPA* and relevant policies and procedures, and of the consequences for non-compliance. This training includes information about:

    - WRH's expectations when it comes to collecting, using or disclosing PHI;

    - the circumstances in which access to PHI is appropriate and inappropriate;

    - the concept of circle of care;

    - appropriate searches and use of the shared EHR system; and

    - that accessing patient PHI when it is not required to provide care to a patient or to perform work duties is a privacy breach.

- At the conclusion of training, staff were required to acknowledge that they are aware of WRH's policies and procedures respecting privacy, confidentiality and security of PHI and that they understand their responsibility to comply with them.

- The shared EHR system used by WRH displayed privacy warning messages on the login/access screens to remind users each time they log on of the restriction against accessing PHI of patients outside the user's circle of care.

- WRH provided its staff with access to the shared EHR system based on their role.

- WRH reviewed its policies and practices on an ongoing basis to ensure they remain reasonable.

Representations of WE Kidz

[47] By contrast, when asked whether it had any reasonable measures to protect PHI in its custody or control at the time of the breach, WE Kidz submitted that it "immediately asked Dr. Afandi to stop collecting, using or disclosing any PHI". It then went on to refer to measures it has since implemented, including a privacy policy and confidentiality agreement, but these were only put in place after the breach. When asked about conditions or restrictions on Dr. Afandi's ability to collect, use, disclose or retain PHI when acting as its agent, WE Kidz conceded that it did not have conditions or restrictions imposed on Dr. Afandi at the time of the incident.

Analysis and findings

[48] The IPC has held that section 12(1) of *PHIPA* requires a custodian to take steps that are reasonable in the circumstances to protect PHI in its custody or control against "unauthorized use or disclosure", among other things.[6] This includes administrative, technical and physical measures or safeguards, including privacy policies, procedures and practices, audit functionality, as well as privacy training and awareness programs and initiatives and annual confidentiality agreements.[7] Further, section 12(1) requires custodians to review their measures or safeguards from time to time to ensure that they continue to be reasonable in the circumstances to protect PHI in their custody or control.[8] This office has stated that the standard in section 12(1) is "reasonableness". It does not require perfection, and the section does not provide a detailed prescription for what is reasonable.[9]

[49] Similarly, section 17(3)(a) of *PHIPA* requires custodians to take steps that are reasonable in the circumstances to ensure that no agent of the custodian collects, uses, discloses, retains or disposes of PHI unless it is in accordance with section 17(2). Among

---

[6] Order HO-013.
[7] PHIPA Decision 204, 2023 CanLII 28868 (ON IPC)
[8] Order HO-010 and PHIPA Decision 204, *Ibid*.
[9] PHIPA Decision 74, 2018, CanLII 78841 (ON IPC), PHIPA Decision 153, 2021 CanLII 70445 (ON IPC)

other things, section 17(2) states that an agent of a custodian can only collect, use, disclose, retain or dispose of PHI if it is not contrary to *PHIPA* or another law.

[50] Lastly, section 11.1 of *PHIPA* requires that custodians take steps that are reasonable in the circumstances to ensure that PHI is not collected without authority.

[51] In regard to WRH, I find that, at the time of the breach, it had reasonable measures in place to protect PHI in its custody or control. I accept that it had in place the essential bones of a robust privacy governance program, including privacy policies and procedures, which it reviewed on an annual basis, and through these policies and procedures ensured its professional staff were clearly aware of the consequences of non-compliance. I accept that WRH also required its professional staff to make annual confidentiality undertakings and participate in annual privacy training. I further accept that WRH conducted and continues to conduct random and ad-hoc audits of accesses to PHI on an ongoing basis, ensures that the EHR displays privacy warnings at the time of user login, and regulates access to the EHR system based on role.

[52] Accordingly, I find that at the time of the breach, WRH had reasonable privacy measures in place in compliance with *PHIPA* sections 12(1), 17 and 11.1.

[53] In contrast, with respect to WE Kidz, I find that, at the time of the breach, it sorely lacked any of the essential elements of a data privacy and security governance program. In fact, upon opening its doors for business, the evidence demonstrates that it had no privacy management program at all. We Kidz' complete lack of documented privacy policies, practices and procedures was plainly not reasonable in the circumstances. It did not take reasonable steps to ensure that:

- PHI is protected against theft, loss and unauthorized use or disclosure,
- no agent of We Kidz collects, uses, discloses, retains or disposes of PHI unless it is in accordance with subsection 17(2) of PHIPA, and
- PHI is not collected without authority.

[54] Accordingly, I find WE Kidz was in breach of its obligations under sections 12(1), 17 and 11.1 of *PHIPA*.

Issue B: Did WRH and WE Kidz have information practices in place, and did they comply with those information practices?

[55] *PHIPA* requires custodians to have in place information practices consistent with the legislation and to comply with those information practices. Specifically, section 10 requires as follows:

> 10(1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations.
>
> 10(2) A health information custodian shall comply with its information practices.

[56] Section 2(1) of the *Act* defines "information practices" as follows:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> > (a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
> >
> > (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information[.]

Representations of the Hospitals

[57] The Hospitals, including WRH, submitted that they had information practices in place at the time of the breach. In support of their submission, the Hospitals provided me with copies of several documents, the most relevant of which are the following:

- The 2022 Regular Members Service Agreement between the Hospitals and TSSO dated January 2022
- The WRH By Law (126 pages), effective July 18, 2024
- The WRH Privacy Policy (originating date November 19,2004, last revised date June 23, 2023)
- The WRH Confidentiality Agreement, signed and dated by Dr. Afandi, July 10, 2020
- TSSO Remote Access Agreement, signed and dated by Dr. Afandi, July 27, 2020
- The WRH Annual Learning Review, Privacy and Confidentiality Course, dated 2022/23, with interactive questions throughout to quiz users on their understanding as well as a copy of the WRH Confidentiality Agreement that users are asked to read carefully and attest to having understood and agreed to its terms by pressing "Submit button" at the end
- The WRH Electronic Monitoring Policy (originating date October 11, 2022, next review date October 11, 2023)

- Copy of the warning flag that appears to users upon login/sign on to the EHR system reminding them of their obligations under *PHIPA* and of the terms and conditions of using the system, including requirements regarding use of passwords and to close and log off the system upon completion

- Screenshot of Dr. Afandi's Learning Journey showing completion of "e-VOLVE Introduction Journey V2" on October 19, 2020; addition of "e-VOLVE Introductory Journey V4" marked completed but undated; addition of e-VOLVE Provider Journey", marked enrolled, but not completed.

- Copy of Dr. Afandi's signed applications for appointment in 2020, and for reappointment, dated July 22, 2022; October 3, 2023; and April 1, 2024.

Representations of WE Kidz

[58] In its representations, WE Kidz confirms that it did not have any information practices in place at the time of the breach.

Analysis and findings

[59] As explained above, section 10 of *PHIPA* requires custodians to have in place information practices that comply with the requirements of the *Act* and its regulations. To satisfy this provision, a custodian must not only have information practices describing when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of PHI, as well as the safeguards with respect to that information, it must also comply with its own practices. In short, under section 10 of *PHIPA*, custodians have to say what they will do, and then do what they say.

[60] Therefore, when a custodian's compliance with section 10 is being questioned by my office, I will not only ask to see the policies, practices and procedures that are in place, but also ask custodians to show that they have, in fact, complied with them. In many ways, this is similar to the concept of *demonstrable accountability* that has been emerging in the data regulatory context in recent years.

[61] Demonstrable accountability refers to a repeatable and demonstrable system of data governance whereby organizations can show regulators more concretely, backed by evidence, how they meet their legal requirements in practice. This notion of demonstrable accountability is intended for organizations to close the trust gap with regulators and with individuals. The concept of demonstrable accountability has evolved in recent years to extend beyond merely checklist compliance, to being able to show that the accountability mechanisms in place are actually working as intended to provide reasonable protection.[10]

[10] *Privacy Act Modernization: A Discussion Paper,* Department of Justice, Canada; *Demonstrating and Measuring Accountability: A Discussion Document, Accountability Phase II – The Paris Project,* October

[62] In this regard, through its submission, WRH appeared to have some difficulty in providing detailed evidence of its compliance with its information practices. Ultimately, while I find that WRH took reasonable steps to protect PHI in its custody and control in these circumstances, and that WRH generally did comply with its own information practices based on undisputed facts, the evidence it submitted to demonstrate these facts was spotty at times. As such, I have provided some examples and recommendations to assist WRH, and other custodians, put forward their best evidence to better demonstrate adherence to their own information practices.

[63] First, many of the WRH policies submitted in support of its position that it had the requisite information practices in place were dated inconsistently. Some included an original date on which the policy took effect, the date of its last revision, the date of its last review, and the date on which the next review would become due. Other policies lacked any such detail. Most notably, the WRH by-law on which WRH heavily relies as having set out the conditions for Dr. Afandi's application for privileges and renewals, is simply marked as having an "Effective date of July 18, 2024". This would seem to contradict WRH's position that the by-law was in effect at the time of Dr. Afandi's original application in 2020 and renewal applications in 2022, 2023 and 2024. In this case, I can reasonably infer that the by-law preceded these application forms given the many explicit references to the by-law in these forms and Dr. Afandi's annual acknowledgement of having read and understood it. In the future, however, I recommend that WRH clearly document the dates on which its by-law was originally adopted and subsequently renewed. The same goes for all other hospital policies and procedures. Ensuring that all policies and procedures have clearly documented dates would enhance WRH's ability to demonstrate compliance with its information practices as they existed at a particular point in time.

[64] Second, WRH provided evidence of Dr. Afandi's signature acknowledging his obligations under the Remote Access Agreement. While there is a signature appended to "the Applicant's signature" dated July 27, 2020, for all intents and purposes, the signature is completely illegible. Again, while I am prepared to reasonably infer that this was indeed Dr. Afandi's signature since he did not contest the Hospitals' submission on this point, it should not be incumbent on the regulator to fill in these gaps. To be able to *demonstrate* that their information practices comply with *PHIPA*, I recommend that WRH provide a place on their forms for the signatory to write their name next to their signature for proper record keeping purposes.

[65] Third, when asked to demonstrate that Dr. Afandi underwent privacy training, WRH submitted a screenshot of a one-page document entitled, "Omar Afandi Learning Journey Completion". This document, by itself, is wholly unclear as to whether Dr. Afandi actually underwent privacy training, what training he completed, and when. Again, while it is not disputed that Dr. Afandi received some training, and I accept that he did, a

---

2010, The Centre for Information Policy Leadership; *The Movement Towards Demonstrable Accountability - Why it Matters,* December 2020, The Information Accountability Foundation.

custodian should be able to provide better evidence of this. I recommend that WRH maintain a clearer record tracking each agent's annual training requirements, including the courses required, courses enrolled in, courses taken, and dates of successful completion each year.

[66] Fourth, WRH submitted that it requires its professional staff to sign a confidentiality agreement upon hiring and annually thereafter, acknowledging that they had read, understood and commit to maintaining WRH's confidentiality expectations at all times. However, other than the confidentiality agreement signed by Dr. Afandi, dated July 10, 2020, WRH has not provided evidence demonstrating that Dr. Afandi renewed this confidentiality undertaking annually. In fairness, the last few slides in WRH's annual privacy training slide deck appear to reproduce the contents of the confidentiality agreement and require that all participants acknowledge that they "have read, understood and commit to maintaining at all times, the Confidentiality expectations outlined within the Confidentiality Agreement" by pressing a "Submit" button to show their acknowledgement and confirm the veracity of that statement. However, again, WRH's documentation showing that Dr. Afandi completed this annual training each year (which should have also included confirmation of his renewed confidentiality undertaking) was not self-evident. This made demonstrating compliance with their information practices more difficult than it needed to be. I recommend that WRH take measures to be able to better demonstrate that its professional staff do in fact renew their confidentiality commitments on an annual basis.

[67] Finally, in its submissions, WRH relies heavily on the fact that Dr. Afandi was made aware of, and agreed to, his confidentiality obligations as a member of the professional staff, when he applied for, and sought renewal of, his privileges each year. In his original application of 2020 and reappointment applications dated 2022, 2023 and 2024, I note there is an explicit provision whereby Dr. Afandi is asked to acknowledge his understanding of, and consent to, the following general statement: "I have read and hereby provide all of the undertakings and acknowledgements required of all applicants to the Professional Staff as set out in the By-Law."

[68] The by-law itself is a 125-page document that requires professional staff, applying for appointment and reappointment, to confirm that they have read and will comply with the by-law, the Rules and Regulations, WRH's mission, vision and strategic plan, and its clinical, administrative and human resources policies and procedures, etc. The by-law also requires professional staff to acknowledge that if they do not comply with these or with applicable legislation, this will constitute a breach of their obligations which may result in their privileges being restricted, suspended, revoked, or denied, and depending on the circumstances, they may be reported to the CPSO.

[69] While this provision is enough for any professional staff member to sit up and take notice, the throughline between this clause and their privacy and confidentiality obligations is weak and should be improved. Throughout the by-law there is surprisingly little, if any, reference to the professional staff's privacy and confidentiality obligations as

agents of WRH other than an oblique reference to *PHIPA* in the definition of applicable legislation among a host of other laws, and an indirect reference to WRH's Privacy Policy, presumably -- but not explicitly -- included in the "policies and procedures" applicable to professional staff.

[70] In order for WRH to ensure that its staff are actually aware of what information practices they are required to comply with, I recommend that WRH update its by-law to include more explicit reference to the privacy and confidentiality obligations of its professional staff. The by-law should include a more express reference to the WRH's Privacy Policy, and WRH should provide a copy of this policy to professional staff prior to signing their application or renewal forms.

[71] In the case of WE Kidz, given the absence of any information practices to begin with, WE Kidz was not in compliance with its obligations under sections 10(1) and (2) of *PHIPA.* The fact that the clinic began operating without any privacy management program at all is deeply concerning and is in stark non-compliance with their obligations under *PHIPA*. This case should serve as a cautionary tale for any start up in Ontario's health sector that decides to put the cart before the horse, and begin operating without the necessary privacy policies, procedures and practices in place. Accordingly, I find WE Kidz was in breach of its obligations under section 10 of the *Act*.

Issue C: Did WRH and WE Kidz respond adequately to the privacy breach?

[72] As set out above, section 12(1) *of PHIPA* requires custodians to take "reasonable" steps to protect PHI in their custody or control against unauthorized use or disclosure, among other things. Subsections (2) and (3) of section 12 further provide that where PHI that is in a custodian's custody or control is used or disclosed without authority[11], the custodian must notify affected individuals and report the breach to the IPC in prescribed circumstances. Specifically, sections 12(2) and (3) state:

> 12 (2) Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,
>
> (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
>
> (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

[11] Among other things.

> (3) If the circumstances surrounding a theft, loss or unauthorized use or disclosure referred to in subsection (2) meet the prescribed requirements, the health information custodian shall notify the Commissioner of the theft or loss or of the unauthorized use or disclosure.

[73] The IPC has held that section 12 includes a requirement for custodians to respond adequately in the event of a privacy breach. This includes determining the scope of the breach and containing it, notifying affected individuals and reporting the breach to the IPC (as appropriate), investigating the cause of the breach, and taking necessary remedial measures to minimize the risk of any similar breach re-occurring.[12] Again, the standard in section 12(1) is "reasonableness".[13]

Representations of WRH

[74] As per the undisputed facts above, WRH was made aware of the patient complaints made to CKHA on May 7, 2024. On the same day, WRH's Chief of Staff called Dr. Afandi and directed him to immediately cease his practice of accessing PHI of individuals who were not his patients and to stop soliciting patients for circumcision services at WE Kidz. Dr. Afandi agreed to do so.

[75] Upon learning of the unauthorized access, WRH, together with CKHA, directed TSSO to conduct an investigation of the shared EHR system to confirm the scope of the PHI that had been inappropriately accessed and to confirm that no other physician had conducted similar searches.

[76] On May 15, WRH states that its Chief of Staff advised Dr. Afandi that, as a result of his unauthorized collection and use of PHI, he would be immediately removed from the on-call schedule for the remainder of his locum appointment (expiring May 31, 2024) and would no longer be permitted to exercise his privileges effective that same day. WRH submitted that it gave Dr. Afandi the opportunity to withdraw his application for reappointment for 2024-2025, which Dr. Afandi agreed to do the next day.

[77] The Hospitals reported the breach to the IPC on May 31, 2024, and notified affected individuals via postal mail the week of July 2, 2024.

[78] WRH submitted that since learning of the breach, together with the other hospitals, it has worked with TSSO to develop and implement the following policies that apply to all users of TSSO's network, including users of the shared EHR system. WRH submits that these policies relate to:

---

[12] See the IPC guidance document "Responding to a Health Privacy Breach: Guidelines for the Health Sector" available online at https://www.ipc.on.ca/en/resources-and-decisions/responding-health-privacy-breach-guidelines-health-sector.
[13] See PHIPA Decision 153, 2021 CanLII 70445 (ON IPC).

- Regional Data Storage and Internal Sharing
- Regional Cyber Security and Privacy Training
- Regional Data Governance Policy
- Regional Data Back-up and Recovery Policy

[79] Moreover, the Hospitals, including WRH, say they are reviewing all existing policies and procedures in place that relate to the governance and operation of the shared EHR to ensure they reflect current best practices, including guidance from the IPC.

[80] The Hospitals, including WRH, submitted they have stepped up mandatory privacy, confidentiality and cybersecurity training that specifically addresses maintaining privacy within the shared EHR system. They submitted that they are working with TSSO to enhance their ability to detect and identify anomalous user activity on a timely basis. They are also considering whether they can limit the functionality of the search feature to avoid overbroad searches (e.g. by gender and date of birth) and eliminate certain demographic data that are initially visible as part of the search results, such as patient name, phone number, and address.

Representations of WE Kidz

[81] WE Kidz submitted that upon learning of Dr. Afandi's actions, it immediately asked him to stop collecting, using or disclosing any PHI. WE Kidz also submitted that "(g)iven the breach did not occur at WE Kidz Pediatrics… no other steps were taken." We Kidz further submitted that it did not otherwise impose any conditions or restrictions on Dr. Afandi at that time.

[82] WE Kidz stated that given affected individuals had already been notified by the Hospitals, WE Kidz did not notify any affected individuals. WE Kidz submitted that it "only has phone numbers of 17 confirmed cases (by text message) and cannot confirm how many of the 74 numbers contacted by phone were related to the privacy breach." Moreover, WE Kidz submitted that it was advised by its legal counsel not to contact any individuals to prevent further unauthorized contact.

[83] WE Kidz submitted that, since the breach, it has taken the following steps to protect PHI in its custody or control from unauthorized use or disclosure:

- created a Privacy Policy,
- created a confidentiality agreement and asked all agents and employees to read and sign it,
- implemented privacy training through Ontario MD for all of its agents and employees,

- implemented physical safeguards, including screen protectors, ensuring their EMR system is locked between patients and limit access to the EMR by role,
- implemented secure messaging with patients, and
- started performing scheduled audits every 6 months as of September 2024, allowing it to see who logged into patient charts and when, so it can make sure agents are only accessing charts they require for providing care and/or for required communications.

[84] WE Kidz further submitted that since the breach, Dr. Afandi has undertaken a number of privacy and security training courses to build his awareness and learn from this experience. Dr. Afandi has also participated in four coaching sessions with a coach on Professionalism and Ethics recommended by the CPSO.

Analysis and Findings

[85] On the whole, I find that WRH responded adequately to the breach but WE Kidz did not. I find that WRH responded in a timely, methodical and responsible manner. It took immediate steps to contain the breach, determine its scope, notify affected individuals, report the breach to my office, investigate the cause of the breach and undertake remedial measures to mitigate chances of such a breach from recurring.

[86] In contrast, I find that WE Kidz' response was not in compliance with *PHIPA*. Rather, the evidence before me demonstrates that WE Kidz was completely unprepared to deal with a breach of this nature, largely due to the fact it had no privacy breach response protocol in place.

[87] I acknowledge WE Kidz' submission that it has taken some remedial steps since the breach to put in place the necessary building blocks of a privacy management and accountability framework. Although WE Kidz has adopted some basic privacy policies and procedures, its submissions suggest a continuing lack of understanding of the purpose for these policies and procedures, a lack of appreciation for the potential consequences of breaching them, and, most fundamentally, an inadequate organizational culture to implement them.

[88] For example, it is revealing that WE Kidz emphasized at least twice in its submission a specific clause in the confidentiality agreement that was developed and signed by Dr. Afandi following the breach. This clause reads:

> I agree that I will not use WE Kidz Pediatrics' phone number to contact patients or families not currently rostered or referred to WE Kidz Pediatrics. If I need to contact a patient or family seen at another facility, I will use that facility's phone number to contact them.

[89] In my view, the phone used to contact patients is completely secondary to the

legal authority of a custodian or its agent to use PHI in its custody or control to contact individuals in the first place. This seeming lack of understanding of its obligations with respect to PHI on the part of WE Kidz is concerning.

[90] Moreover, in its submission, WE Kidz stated that "there was no physical or potential harm because of the contraventions". This too seems to reveal a fundamental lack of appreciation of the potential emotional or other impacts on patients resulting from the custodian's failure to comply with its basic privacy and confidentiality obligations.

[91] While WE Kidz has taken steps since the incident to create policies and procedures to address its prior shortcomings, its representations to my office suggest that it would benefit from further learning. For these reasons, I recommend that, as part of a broader privacy management and accountability framework, WE Kidz strengthen its privacy policies and procedures and that its management and staff undergo further privacy training. In strengthening its privacy policies and procedures, WE Kidz is encouraged to consider the IPC's *Privacy Management Handbook for Small Health Care Organizations*.[14]

Issue D: Given the circumstances of this matter, should the IPC impose AMPs or any other order against Dr. Afandi and/or WE Kidz?

[92] Effective January 1, 2024,[15] sections 61(1)(h.1) and 61.1 of *PHIPA* and section 35 of the accompanying regulation, O. Reg. 329/04 (the regulation), provides my office with a new authority to order the payment of AMPs against a custodian or any other person that has contravened *PHIPA* or its regulation in cases that warrant it.

[93] The stated purposes of this new statutory power are to: (a) encourage compliance with *PHIPA* and its regulations; or (b) prevent a person from deriving, directly or indirectly, any economic benefit as a result of a contravention of *PHIPA* or its regulations.[16] I note that these purposes for AMPs are not intended to be punitive – and I am mindful not to consider punishment of Dr. Afandi or WE Kidz as a reason to impose an AMP.

[94] On the same date as the coming into force of this new authority, my office issued guidance for the health sector: *Administrative Monetary Penalties: Guidance for the Health Care Sector* (the IPC's AMPs guidance).[17]

[95] This guidance describes the general approach my office will adopt in interpreting and applying this new enforcement power:

---

[14] https://www.ipc.on.ca/en/resources/privacy-management-handbook-for-small-health-care-organizations

[15] This is the date the AMP regulations under *PHIPA* came into force.

[16] See section 61.1(1) of *PHIPA*.

[17] https://www.ipc.on.ca/en/resources-and-decisions/administrative-monetary-penalties-guidance-health-care-sector

> AMPs are part of the IPC's broader regulatory toolkit for encouraging compliance with *PHIPA* in a manner that is flexible, balanced, and progressive. The IPC's ability to directly impose AMPs provides additional flexibility to address contraventions of *PHIPA* with appropriate and meaningful consequences, depending on their level of severity. AMPs are but one option among the range of escalating actions and interventions available to the IPC, short of referring offences to the Attorney General of Ontario for prosecution.
>
> The IPC takes a measured and proportionate approach to assessing the most appropriate way of addressing each contravention. Similar to the values and principles underlying a just culture approach, we apply our statutory responsibilities in a way that balances the need for accountability and continuous learning. A just culture approach generally emphasizes the value of openly reporting and learning from medical errors that occur in complex systems, while reserving more severe consequences for cases where stronger interventions are necessary to ensure proper accountability.

[96] The IPC's AMPs guidance goes on to describe the kinds of situations in which AMPs might be appropriate. Without limiting other possible types of cases or scenarios, the guidance references the following situation:

> **Contraventions for economic gain**: In previous cases before the IPC, agents of a hospital were found to be accessing patient records and improperly using and disclosing personal health information without authority for the purpose of selling products or services related to the information. If similar cases were to come before the IPC after January 1, 2024, the IPC could consider imposing AMPs where appropriate to prevent the agent from directly or indirectly deriving any economic benefit as a result of contravening *PHIPA*.

[97] With respect to the quantum of an AMP, section 35(1) of the regulation prescribes that the maximum amount of AMP I may impose against Dr. Afandi, being a natural person, is $50,000, whereas the maximum AMP that I may impose against WE Kidz, as a non-natural person, is $500,000.[18] Despite these limits, section 35(2) of the regulation provides that I may increase the amount of an administrative penalty that a person is required to pay by an amount equal to the economic benefit acquired by, or that accrued to, the person as a result of the contraventions.[19]

[98] In determining the appropriate amount of AMP to impose, I have considered the statutory purposes of AMPs, i.e. encouraging compliance with *PHIPA* (and its regulations) or preventing a person from deriving, directly or indirectly, any economic benefit as a

[18] O. Reg. 329/04, section 35(1).
[19] O. Reg. 329/04, section 35(2).

result of a contravention of *PHIPA* (or its regulations).

[99] I have also considered the criteria set out in section 35(3) of the regulation[20]:

1. The extent to which the contraventions deviate from the requirements of the Act or its regulations.

2. The extent to which the person could have taken steps to prevent the contraventions.

3. The extent of the harm or potential harm to others resulting from the contraventions.

4. The extent to which the person tried to mitigate any harm or potential harm or took any other remedial action.

5. The number of individuals, health information custodians and other persons affected by the contraventions.

6. Whether the person notified the Commissioner and any individuals whose personal health information was affected by the contraventions.

7. The extent to which the person derived or reasonably might have expected to derive, directly or indirectly, any economic benefit from the contraventions.

8. Whether the person has previously contravened the Act or its regulations.

[100] This same regulation also provides that I may consider any other criteria I consider to be relevant.[21]

[101] In my Notice of Review, I put all parties on notice that I intended to assess, and decide, whether an AMP should be imposed on Dr. Afandi and/or on WE Kidz in this case and if so, in what amount. I sought submissions from all parties on this issue.

Representations of the Hospitals, including WRH

[102] The Hospitals, including WRH, submitted that, in their view, the issuance of an AMP against Dr. Afandi and/or WE Kidz would be appropriate to deter "future potential rogue actors" who have access to PHI in the course of providing patient care, from inappropriately accessing and using PHI including for their own economic gain. In this case, the Hospitals state that Dr. Afandi was aware of his obligations under *PHIPA* and breached them when he could have avoided doing so. They state that some patients were very disturbed by Dr. Afandi's conduct and appear to have suffered emotional harm. Moreover, they submit that Dr. Afandi derived direct economic benefit from his

[20] O. Reg. 329/04, section 35(3).
[21] O. Reg. 329/04, section 35(3).

contravention.

[103] Given the media attention this incident has received, the Hospitals submit that an AMP may help rebuild any public trust lost as a result. Further, the Hospitals submit that Dr. Afandi's unauthorized accesses have resulted in "tremendous" cost to the Hospitals (and therefore the public) in terms of the resources required to investigate and deal with the incident. They submit therefore, it would be appropriate to impose at least some financial penalty on Dr. Afandi in this case. The Hospitals acknowledge, however, that Dr. Afandi promptly agreed to cease his unlawful conduct when it was brought to his attention. Ultimately, the Hospitals submit that they defer to my discretion on whether AMPs should be imposed against either Dr. Afandi or WE Kidz, or both.

Representations of Dr. Afandi

[104] It is clear from Dr. Afandi's representations that he has acknowledged his wrongdoing. He submits, and the parties do not dispute, that he immediately ceased this practice when he was confronted by the Chief of Staff about it. Additionally, from his representations it appears that he is genuinely remorseful.

[105] Dr. Afandi submits that the accesses to the shared EHR system did not involve opening the charts but were limited to viewing basic demographic information about eligible patients and inputting their phone numbers into his Weave application. He submits that the actual number of patients he would have proceeded to contact would have been much lower than the number of phone numbers recorded. Dr. Afandi maintains that the maximum number of affected patients he contacted was potentially 91 (74 telephone contacts and 17 text messages) over a period of 18 days (between April 20 and May 7), although several of these telephone calls may have been made to his regular patients for purposes unrelated to the breach.

[106] As I indicated at the beginning of this decision, Dr. Afandi requested, and I agreed, to keep confidential from the Hospitals some of his representations to ensure his full participation in my review. Some of the representations I agreed to withhold relate specifically to the imposition of an AMP against Dr. Afandi, and although I have not reproduced them here, I have carefully considered them.

Representations of WE Kidz

[107] For its part, WE Kidz submitted that I should not impose an AMP against either it or Dr. Afandi in this case. WE Kidz submitted that prior to this incident, Dr. Afandi had no contraventions. WE Kidz further submitted that the amount of money Dr. Afandi and WE Kidz gained through Dr. Afandi's unauthorized accesses of PHI was not significant. WE Kidz submitted that Dr. Afandi charged $350 for each procedure and out of that, paid $35 to WE Kidz as an overhead charge. WE Kidz submitted that at most, Dr. Afandi would have earned $700 from his unauthorized access of PHI (if one includes the patient he "solicited" while on rounds at WRH) and of this, WE Kidz would have made $70.

Therefore, according to WE Kidz, if I am to impose an AMP, I should impose an AMP of a modest sum equal to $630 against Dr. Afandi and $70 against WE Kidz for the economic gain each received as a result of the breach.

[108] WE Kidz submitted that, since this breach, Dr. Afandi has readily undergone all the necessary remedial action, including taking several courses to build awareness of his obligations under *PHIPA,* and undergoing at least four sessions of coaching with a professional coach on Professionalism and Ethics.

[109] WE Kidz submitted that it believes it has since taken the necessary steps to prevent any similar unauthorized access and use of PHI from occurring in the future.

[110] WE Kidz maintains that there was no physical harm or potential harm to patients because of Dr. Afandi's unauthorized access and use of PHI.

Analysis and Findings on Whether to Impose AMPs

[111] I have carefully considered all the above facts and parties' submissions in this case. I have decided that this is an appropriate case for ordering AMPs against both Dr. Afandi and WE Kidz. I have considered first and foremost what the legislature has stated should be the statutory purposes of administrative penalties under *PHIPA*, namely, to encourage compliance with *PHIPA* and its regulations, or to prevent a person from deriving, directly or indirectly, any economic benefit as a result of a contravention. I find both such purposes would be served by the imposition of AMPs in this case.

[112] The evidence demonstrates that Dr. Afandi inappropriately accessed the shared EHR system he had access to as an agent of WRH for the purpose of identifying eligible patients to whom he could sell his services of performing circumcision procedures privately through his clinic, WE Kidz. By accessing and using this information, Dr. Afandi was seeking to derive, *or reasonably might have expected to derive*, an economic benefit above what he would earn as a professional staff member at WRH. In any event, Dr. Afandi's motivation to obtain an economic benefit is not a pre-condition for imposing an AMP. The fact of the matter is, through Dr. Afandi's contravention of *PHIPA*, he obtained an economic benefit and reasonably might have expected to continue deriving additional economic benefits had he not been called out on this practice and asked by WRH to stop immediately.

[113] Dr. Afandi stated that he was unaware that his practice of accessing patients' PHI through the shared EHR for the purposes of soliciting them for circumcision services was contrary to his privacy and confidentiality obligations under *PHIPA*. In my view, this position is not tenable. Any reasonable health professional should have known that such a practice was not appropriate or was at least sufficiently questionable that, prior to engaging in such practice, he should have sought advice from WRH's administrators, lawyers, ethics committee or other advisors. Regardless, knowledge of the law is not a condition precedent for imposing an AMP.

[114] Regarding WE Kidz' conduct in this case, I find that its level of disregard for patients' privacy rights and its obligations as a health information custodian under *PHIPA* also makes this an eligible case for an AMP order.

[115] In this case, the evidence is clear that WE Kidz opened its doors for business as a pediatric clinic and began welcoming new patients without having any privacy management program in place. Not only is this contrary to *PHIPA,* it also runs contrary to the very basic professional obligations of custodians to protect the privacy and confidentiality of their patients. By any reasonable standard, privacy and security of its patients should have been part of the WE Kidz' launch plans. As a result of this significant lapse, Dr. Afandi was enabled in his ability to contravene *PHIPA* and derive economic benefit of which he shared a portion with WE Kidz. Although the amount gained by WE Kidz was relatively minimal in this case, it reasonably might have expected to continue deriving economic benefits from this arrangement in the future.

Quantum of AMP to be imposed on Dr. Afandi

[116] In determining the amount of the AMP I will order against Dr. Afandi in this specific case, I have considered the following, based on the criteria set out in section 35(3) of the regulation to *PHIPA*:[22]

1. Dr. Afandi's unauthorized accesses to the shared EHR system for the purpose of identifying and contacting patients eligible for circumcision services at his private clinic deviated significantly from his obligations and authorities as an agent of WRH under *PHIPA*.

2. Dr. Afandi could have easily taken steps to avoid these contraventions. They were entirely of his own doing and volition. Although he claims he did not know his accesses to PHI in the shared EHR system contravened *PHIPA*, in my view, any reasonable health professional would have at least questioned whether his actions were appropriate and in compliance with both the law and hospital policy and would have consulted others accordingly. Had he consulted prior to accessing PHI through the EHR system, he would have received appropriate advice on his obligations under *PHIPA* and been warned against proceeding on this path.

3. The harm to patients outside Dr. Afandi's circle of care, is not to be underestimated. These patients had just given birth and could have been in a vulnerable emotional state. Being disturbed by someone out of the blue who would have contacted them by phone to offer circumcision services at a private clinic could have left many of them highly perturbed, questioning how such a physician, unrelated to their care, got access to their phone number and other PHI in the first place. This was exactly the reaction of at least two women who were clearly upset

[22] O. Reg. 329/04.

and complained to the Hospitals about it. I find that there was some actual harm to these patients and potentially to other patients as well.

4. Although Dr. Afandi did not try to mitigate the harms at the time he was soliciting patients, I accept that he immediately ceased this practice when he was advised of his breach of *PHIPA* and directed to stop by WRH's Chief of Staff. He willingly and readily completed all of the necessary privacy and security training since and participated in remedial coaching sessions to learn from this situation.

5. According to the TSSO investigation, Dr. Afandi queried the EHR system by sex and date of birth 146 times through which he was able to access and view the PHI of potentially 831 patients. While this is a significant number of individuals, it is partly mitigated by the fact that there is no evidence that Dr. Afandi viewed the patients' charts. By his own admission, between April 20 and May 7, 2024, Dr. Afandi used the PHI of potentially up to 91 individuals to contact them by phone or by text for the purpose of soliciting circumcision services offered at WE Kidz, though some of these calls may have been to his own patients.

6. Dr. Afandi himself did not notify affected individuals of his contraventions. The Hospitals carried out the notification, as was appropriate in this case. However, Dr. Afandi did not notify the IPC of this matter either.

7. According to WE Kidz' submissions, the most Dr. Afandi would have gained economically from this venture is $630 (equal to two procedures at a cost of $350 each, less $70 paid to WE Kidz as overhead).[23] Although this amount of economic benefit may seem relatively modest, the regulations require me to consider the extent to which Dr. Afandi derived or *reasonably might have expected to derive*, directly or indirectly, any economic benefit from the contraventions. I have reason to believe that these contraventions would have continued had they not been reported by patients and had WRH not directed Dr. Afandi to stop immediately. It would appear from the cold-calling and texting method employed by Dr. Afandi, that he reasonably might have expected to derive an economic benefit significantly higher than the amount he actually earned before these contraventions became known and quickly ceased.

8. There is no evidence before me that Dr. Afandi has previously contravened *PHIPA* or its regulations.

[117] For the above noted reasons, I have determined that an administrative penalty of $5,000 against Dr. Afandi is warranted in this case. I believe it is a reasonable amount to encourage Dr. Afandi and others to respect their obligations under *PHIPA* and to discourage him and others from attempting to unlawfully gain access to patients' PHI for

[23] And I note this amount includes the one patient he "solicited" while on rounds at WRH, and that I have not addressed in this decision.

direct or indirect economic gain in the future.

Quantum of AMP to be Imposed on WE Kidz

[118] In determining the amount of the AMP I will order against WE Kidz in the circumstances of this specific case, I have considered the following based on the criteria set out in section 35(3) of the regulation to *PHIPA*:[24]

1. WE Kidz' deviation from its obligations under *PHIPA* was significant in this case. When WE Kidz opened its doors for business, it had no privacy management program to speak of. It indicated in its representations that it had no information practices and imposed no limits on Dr. Afandi's authority to collect, use or disclose PHI which enabled Dr. Afandi's contraventions in this case.

2. WE Kidz could have easily taken steps to prevent these contraventions. In compliance with its obligations under *PHIPA,* it should have taken the necessary time and expended the minimal effort required to set up at least the foundational building blocks of a privacy management program before commencing operations. Even recognizing that a robust privacy management program matures and becomes more sophisticated over time, in this case WE Kidz started operating without even a base level privacy management program.

3. As mentioned above, the emotional harm or potential for such harm to patients in this case was significant. The fact that WE Kidz submits there were no physical harms that resulted from Dr. Afandi's unauthorized actions with respect to PHI, without any recognition of the potential emotional harms to mothers of newborn infants is particularly concerning. In my view, this shows a failure on WE Kidz' part to acknowledge, let alone understand, potential emotional harm to patients resulting from the unauthorized use of the PHI they entrusted to one of its agents.

4. Although WE Kidz did take steps to remediate its breach of its obligations under *PHIPA* by putting in place the basic components of a privacy management program after the fact, its emphasis on such a secondary aspect of its new confidentiality agreement (which phone to use), leads me to question WE Kidz' understanding of its responsibilities as a custodian under *PHIPA*, and further question how robust the remedial measures it has put in place really are.

5. The exact number of phone numbers Dr. Afandi in appropriately accessed and used to call or text patients while acting as agent of WE Kidz is not clear. While the number of affected individuals is a factor to consider, it is not determinative. From Dr. Afandi's own submissions, he contacted, by text or by phone, 91 individuals, some of whom were outside of his circle of care.

[24] O. Reg. 329/04.

6. WE Kidz did not notify the affected individuals of Dr. Afandi's contraventions. WE Kidz relied on the fact that the Hospitals had done so, and on advice of its legal counsel decided not to notify due to the risk of further contravening the affected individuals' privacy. While it may have been appropriate in this case to rely on the Hospitals to notify individuals, WE Kidz did not notify the IPC.

7. WE Kidz submitted that if I decide that an AMP is warranted against WE Kidz in this case, an appropriate amount would be $70, the amount of overhead WE Kidz would have recuperated from Dr. Afandi for two procedures.[25] However, more relevant in my view in justifying the imposition on WE Kidz of an AMP and its quantum, is WE Kidz' lack of any privacy management program at the time of the breach that enabled Dr. Afandi to violate *PHIPA*.

8. There is no evidence before me that WE Kidz has previously contravened *PHIPA* or its regulations.

[119] For the above noted reasons, I have determined that an administrative penalty of $7,500 against WE Kidz is warranted in this case. I believe it is a reasonable amount to encourage WE Kidz and other start-ups in the health sector to respect and comply with their basic obligations as custodians under *PHIPA* and ensure that these foundational protections are in place prior to commencing their operations. This amount will also prevent WE Kidz and discourage other custodians from obtaining or enabling any economic benefit to be derived from such contraventions.

Other Order - Secure Disposal of Personal Health Information

[120] Dr. Afandi indicated he has retained for "investigative purposes" the logs of messages and phone calls he made in connection with this matter, the telephone numbers of the individuals he contacted, and the PHI relating to individuals on whom he performed circumcisions. I asked the parties whether I should order Dr. Afandi and WE Kidz to securely dispose of this information. In response, WE Kidz submitted:

> WE Kidz Pediatrics will be deleting all data, including phone numbers, of PHI collected once the IPC and CPSO investigations are completed. Given the discrepancy between Dr. Afandi's actions and what is reported by WRH, the data audit is a very important piece of evidence WE Kidz Pediatrics has in order to prove the extent of the breach is not as reported by WRH.

[121] I have also considered the confidential representations of Dr. Afandi on this issue.

[122] As I have found above, the collection, use and disclosure of this information by Dr. Afandi (as agent of WE Kidz) and by WE Kidz itself (as relevant custodian), were

[25] Again, I note this amount includes the one patient he "solicited" while on rounds at WRH, and that I have not addressed in this decision.

contrary to *PHIPA*.[26] In light of these findings, I have considered my powers under section 61(1) of *PHIPA* and in particular, paragraph (e):

> 61 (1) After conducting a review under section 57 or 58, the Commissioner may,
>
> […]
>
> (e) make an order directing any person whose activities the Commissioner reviewed to return, transfer or dispose of records of personal health information that the Commissioner determines the person collected, used or disclosed in contravention of this Act, its regulations, or an agreement entered into under this Act but only if the return, transfer or disposal of the records is not reasonably expected to adversely affect the provision of health care to an individual.

[123] In the circumstances of this case, I believe it is appropriate to make an order requiring both WE Kidz and Dr. Afandi to securely dispose of records containing PHI[27] obtained from the shared EHR system and used by Dr. Afandi to offer circumcision services at WE Kidz. There is no evidence before me to indicate that the secure disposal of this information would adversely affect the provision of health care to an individual. Moreover, to ensure that this evidence remains available for regulatory proceedings, this disposal will only be required after the CPSO proceedings (and any applicable timeframe for appeal or judicial review proceedings in relation to this decision and the CPSO matter) have ended. To be clear, this order does not apply to the PHI of individuals on whom Dr. Afandi performed a circumcision that must be retained in compliance with regulatory requirements.

RECOMMENDATIONS FOR WRH:

Pursuant to sections 61(1)(i) and 61(4) of the *PHIPA,* and for the reasons stated above, I make no order against the Hospitals. However, I recommend that WRH:

- ensure that all policies and procedures have clearly documented dates in order to demonstrate compliance with its information practices as they exist at a particular point in time;

---

[26] See section 17 of *PHIPA.*

[27] In the circumstances of this case, and for greater certainty, I find that the logs of messages and phone calls and telephone numbers used by Dr. Afandi are also PHI within the meaning of the *Act* as this information relates to the provision of health care at one of the Hospitals and it is reasonably foreseeable in the circumstances that they could be utilized, either alone or with other information, to identify an individual.

- provide a place on their forms for the signatory to write their name next to their signature for proper record keeping purposes;

- maintain a clear record tracking each agent's annual training requirements, including the courses required, courses enrolled in, courses taken, and dates of successful completion each year;

- take measures to be able to better demonstrate that its professional staff do in fact renew their confidentiality commitments on an annual basis; and,

- update its by-law to include more explicit reference to the privacy and confidentiality obligations of its professional staff. The by-law should include a more explicit reference to WRH's Privacy Policy, and WRH should provide a copy of its Privacy Policy to professional staff prior to signing their application or renewal forms.

ORDERS FOR DR. AFANDI:

Pursuant to sections 61(1) and 61.1 of *PHIPA*, and for the above reasons:

1. I order that an administrative penalty of $5,000 be imposed on Dr. Omar Afandi for the above-noted contraventions of *PHIPA*, to be paid by Dr. Omar Afandi within 30 days of the date of this decision, by cheque to the Ontario Minister of Finance.

   To help facilitate this payment, I understand that the Ontario Ministry of Finance will issue an invoice to Dr. Omar Afandi shortly after the issuance of this order.

2. I order Dr. Omar Afandi to:

   (a) securely dispose of all records containing personal health information obtained from the shared EHR system and used by Dr. Afandi to offer circumcision services at WE Kidz, including all copies of such personal health information in whatever medium they may be maintained, within 60 days of the expiry of the time to appeal or bring an application to judicially review this decision or any decision of the College of Physicians and Surgeons of Ontario in relation to this matter, whichever is longer; and

   (b) provide my office with written confirmation when this secure disposal has been completed.

   For greater certainty, this order does not apply to personal health information of individuals on whom Dr. Afandi performed a circumcision that must be retained according to regulatory requirements.

ORDERS AND RECOMMENDATIONS FOR WE KIDZ:

Pursuant to sections 61(1) and 61.1 of *PHIPA*, and for the above reasons:

1. I order that an administrative penalty of $7,500 be imposed on 1000812873 Ontario Inc. o/a WE Kidz Pediatrics for the above-noted contraventions of *PHIPA* to be paid by 1000812873 Ontario Inc. o/a WE Kidz Pediatrics within 30 days of the date of this decision, by cheque to the Ontario Minister of Finance.

2. To help facilitate this payment, I understand that the Ontario Ministry of Finance will issue an invoice to 1000812873 Ontario Inc. o/a WE Kidz Pediatrics shortly after the issuance of this order.

3. I order that 1000812873 Ontario Inc. o/a WE Kidz Pediatrics (WE Kidz):

(a) securely dispose of all records containing personal health information obtained from the shared EHR system and used by Dr. Afandi to offer circumcision services at WE Kidz, including all copies of such personal health information in whatever medium they may be maintained, within 60 days of the expiry of the time to appeal or bring an application to judicially review this decision or any decision of the College of Physicians and Surgeons of Ontario in relation to this matter, whichever is longer; and

(b) provide my office with written confirmation when this secure disposal has been completed.

For greater certainty, this order does not apply to personal health information of individuals on whom Dr. Afandi performed a circumcision that must be retained according to regulatory requirements.

I recommend that:

- 1000812873 Ontario Inc. o/a WE Kidz Pediatrics strengthen its privacy policies and procedures, and have its management and staff undergo further privacy training. In strengthening its privacy policies and procedures, WE Kidz is encouraged to consider the IPC's *Privacy Management Handbook for Small Health Care Organizations*.[28]

Original Signed by: August 27, 2025

Patricia Kosseim
Commissioner

[28] https://www.ipc.on.ca/en/resources/privacy-management-handbook-for-small-health-care-organizations.