Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 102

HR15-161, HR15-161-2, HR15-161-3, HR15-118, HR15-144 and HR16-1

Three hospitals that are part of a group of health information custodians that share an electronic patient information system

October 30, 2019

Summary: The Information and Privacy Commissioner of Ontario (IPC) received breach reports from three hospitals of unauthorized access by six agents to information contained in a shared electronic patient information system. The hospitals involved in this investigation are part of a group of health information custodians that share access to the same system. The IPC identified ongoing issues relating to the shared system including issues with respect to training, auditing practices, notification practices and agreements. In light of the steps taken by the hospitals, as well as by the larger group that also shares access to the system, to address the issues identified by the IPC, no review of this matter will be conducted under Part VI of the *Personal Health Information Protection Act, 2004*.

Statutes considered: *Personal Health Information Protection Act, 2004*, sections 2, 6(1), 10, 12(1), 12(2), 17,18-20, 29, 36, 37, 38-48, 50, *Ontario Regulation 329/04*, section 6.

Decisions considered: HO-010, HO-13, PHIPA Decision 50

INTRODUCTION:

[1] In 2015, the Information and Privacy Commissioner of Ontario (IPC) received a report from a hospital of unauthorized access by an agent to information contained in a shared electronic patient information system (hereinafter referred to as Meditech or the shared system). The IPC identified issues with the hospital's privacy practices that could not be quickly resolved and, as a result, the file was transferred to the investigation stage of the IPC's process.

[2] At this time, the IPC noted that several different health information custodians (custodians) participating in this shared system had reported privacy breaches to the IPC, over a few years. The IPC decided to examine breaches reported to this office from this particular group of custodians since 2011, with a view to assess whether they raised common and potentially systemic issues across the shared system.

[3] An examination of each of the breaches by the IPC suggested that the custodians participating in the shared system had ongoing issues with respect to training, consistent auditing practices and timely notification of breaches, among other things, that were all related to the shared system and that had not been adequately addressed. As a result, five active breach files, that included six separate breaches at the Intake stage, were transferred to the Investigation stage of the IPC's process and assigned to an investigator to complete an investigation of these six breaches in the shared system.

[4] The IPC has now completed this lengthy and complex investigation involving multiple files and health information custodians. As set out in detail below, significant improvements have been made to the policies and procedures applicable to the shared system during the course of this investigation and, as such, it is not necessary for this investigation to proceed to the adjudication stage of the IPC's processes under the *Personal Health Information Protection Act, 2004* (the *Act*).

SHARED SYSTEMS:

The Benefits and Risks of Shared Systems

[5] Being a part of a shared system can provide many benefits to health information custodians. There are also a number of challenges and problems that can arise when multiple health information custodians participate in a shared system.

[6] In Ontario, when a custodian is part of a shared system the custodian generally does not have sole custody or control of the personal health information in the shared system. A health information custodian typically only has custody or control of the personal health information that the health information custodian creates or contributes to the shared system and the personal health information that the custodian collects from the shared system.

[7] In addition to custody and control generally being shared, accountability for personal health information is also shared. Shared custody and control can pose unique challenges for compliance with the *Act*. For instance, there can be a lack of clarity as to which health information custodian is responsible for undertaking each duty and fulfilling each obligation in the *Act* and its regulations (for example, there can be confusion around which custodian is required to notify the individual of a privacy breach). There can also be a lack of clarity about who is the person subject to the obligations of health information network providers (referenced below).

[8] Additionally, there can be an increased risk of unauthorized use and disclosure because typically all participating health information custodians and their agents have access to all information in the shared system. A shared system can also attract hackers and others with malicious intent given that there is generally a significant amount of information accessible.

[9] When establishing a shared system, health information custodians need to consider the above challenges and ensure that they have a governance framework and harmonized privacy policies and procedures to address them as well as any other issues that may be relevant to their particular situation.

Service Providers and Shared Systems

[10] Health information custodians are permitted by the *Act* to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information.[1] In addition, they may rely on others to provide such electronic means.[2] Persons who provide these services to custodians may, or may not, be an "agent" of the custodian. If they are an agent, they are subject to the obligations imposed by section 17 of the *Act*. If they are not an agent, they are subject to the obligations imposed by section 6(1) of *Ontario Regulation 329/04* made under the *Act*. As the IPC has previously noted, the rules for agent and non-agent electronic service providers reflect the fact that the person who provides services to the custodian is not the decision-maker with respect to the personal health information and acts at the direction of the health information custodian.[3]

[11] The *Act* also regulates persons who provide services to two or more health information custodians where the services are provided primarily to custodians to enable them to use electronic means to disclose personal health information to one another. The *Act* refers to this type of electronic service provider as a health information network provider (HINP). A HINP is subject to additional requirements under section 6 of *Ontario Regulation 329/04*.[4]

[12] When dealing with a HINP or any other person who provides services to enable a custodian to use electronic means to manage personal health information, ultimate responsibility for the personal health information always rests with the custodian.

---

[1] The *Act,* section 10(3).
[2] Ibid. section 10(4).
[3] PHIPA Decision 50 at paras 34-37; see also Halyna Perun, Michael Orr and Fannie Dimitriadis, *Guide to the Ontario Personal Health Information Protection Act* (Irwin Law: Toronto, 2005), 65.
[4] *Ontario Regulation 329/04,* sections 6(2) and (3).

Governance Framework for the Shared System

[13] This investigation involves three hospitals who reported six breaches to the IPC. One of the reported breaches involved a staff member of a fourth hospital. These four hospitals are part of a group of custodians that have agreed to share the Meditech system. This group of custodians signed a Shared Information System Service Agreement (Agreement) governing the terms under which they share the Meditech system.

[14] Among other things, the Agreement establishes a steering committee. The parties to the Agreement appoint individuals to the committee. The steering committee provides strategic direction and authority for the maintenance of the shared system. In addition, this steering committee has the ability to strike working groups.

[15] The group of custodians also has an agreement with four additional health information custodians that allows these custodians access to the shared system. These health information custodians are referred to as "customers". This agreement sets out the terms of the customers' access to the shared system. As part of the agreement, the customer is required to accept the policies, procedures and standards that are developed by the group of custodians. Customers are unable to vote on issues related to the shared system through the steering committee. At the time of this investigation, these customers included medical centres, clinics and a laboratory.

[16] The shared system houses personal health information of patients from all the health information custodians that have access to the shared system; being the group of hospitals and the customers. Agents of the health information custodians that have access to the shared system have potential access to all of the personal health information that is available on the shared system, covering a large geographic area.

[17] All health information custodians participating in the shared system are considered to be the custodian of the personal health information they create or contribute to, or collect from, the system.

[18] Of the partnered hospitals, one hospital (hospital #3)[5] has been identified as the HINP in regards to the shared system. In this sense, hospital #3 wears two hats in the context of this decision – it is a hospital participating in the shared system but it is also a HINP.

[19] The steering committee established a working group called the "Privacy and Policy Working Group" (the working group). The working group has a number of

---

[5] In keeping with the IPC's usual practice for *PHIPA* decisions issued at the investigation stage, this decision does not identify by name the health information custodians who were the subject to this investigation.

responsibilities including identifying and developing policies and procedures for the group of custodians, developing action plans to address issues, reviewing and responding to reports concerning privacy audits conducted as a result of the policies and procedures, monitoring and responding to privacy legislation amendments and regulations and reviewing products and services for privacy implications.

[20] As part of the IPC's investigation, the steering committee, the working group and/or the hospitals who reported breaches to the IPC have undertaken to take a variety of steps to improve the policies and procedures in place to protect personal health information in the shared system (including on behalf of all of the participants in the shared system).

[21] The IPC is grateful for the co-operation these parties have shown in responding to the IPC's investigation, and their willingness to devote much time to resolving the issues raised in these matters.

THE SIX BREACHES:

[22] Under this heading, I summarize the facts of each of the six breaches reported to the IPC as well as the concerns that these reported breaches raised for the IPC. Later in this decision, I describe the steps that have been taken to remedy these concerns.

[23] The details of the six reported breaches at issue in this investigation are as follows:[6]

> **Breach #1:**
>
> Hospital #1 received a complaint that a nurse of the hospital accessed a patient's file without authorization. In response, the hospital completed an audit. The audit identified 60 breaches dating back to 2010 that involved the personal health information of family, friends, high profile patients, an ex-spouse and the ex-spouse's girlfriend. Some of the personal health information accessed was information of a patient that was treated at another hospital. The information was accessed by the nurse through the shared system.
>
> The nurse involved was initially suspended with pay. Subsequently, the nurse was reported to the College of Nurses of Ontario and dismissed. Hospital #1 notified the affected patients.

[6] Breaches 4 to 6 arise out of the same factual circumstances (an audit conducted by Hospital #3 on accesses to the personal health information of two high profile patients).

At the time of the breach, the hospital provided training to agents upon hire but did not provide ongoing annual training to its agents. The hospital required its agents to sign a confidentiality agreement at the time of hire but did not require the agents to re-sign the confidentiality agreement on an annual basis.

Agents of the hospital did not view a privacy notice prior to accessing personal health information on the shared system.

Finally, the hospital completed random audits on a monthly basis and targeted audits as required. The audit reports completed by hospital #1 at the time of the breach did not track the amount of time that a user spent on a particular section of a patients' health record.

Breach #2:

Hospital #2's privacy office received a report pertaining to the Ontario Laboratories Information System (OLIS). Upon review of the report, the hospital determined that a nurse identified on the report viewed a patient's personal health information for whom the nurse was not part of that patient's circle of care. A further audit of the nurse's accesses was completed. The audit showed that the nurse had 144 accesses to personal health information of 21 patients between 2011 and 2015 without authorization, including friends, family and colleagues. Some of the additional accesses identified were also accesses to personal health information of patients who were treated at another hospital.

The nurse involved was suspended with pay and access to the shared system was suspended during the investigation. The nurse was subsequently dismissed and reported to the College of Nurses of Ontario. The hospital notified the affected patients.

At the time of the breach, the hospital provided new hires with privacy training during orientation that occurred on a quarterly basis. If agents were hired before the scheduled orientation date, the agent's manager was to review privacy policies and the confidentiality agreement with the new employee before their start date.

Annual privacy training was not mandatory (but initial privacy training was provided as noted above). Physicians practising at hospital #2 were not provided with any privacy training either initially or annually thereafter.

Hospital #2 required its agents to sign confidentiality agreements upon hire. Confidentiality agreements were to be re-signed at annual performance reviews, however, the hospital advised that it determined that not all performance reviews were completed annually and, as a

result, confidentiality agreements were not consistently re-signed on an annual basis.

At the time of the breach, hospital #2 had a hospital policy that referred to an audit procedure but did not incorporate the requirements contained in the auditing policy developed for the health information custodians with access to the shared system. The shared system auditing policy required that random audits be performed on a monthly basis. Hospital #2 advised that at the time of the breach, it ran random audits of users on a quarterly basis and the audits covered a 3-month period.

Hospital #2 also did not have a privacy notice viewed by its agents prior to accessing personal health information.

As noted above, the initial breach was identified from an OLIS report. Hospital #2's position was that the personal health information accessed through OLIS was not in the custody or control of hospital #2. Hospital #2 explained that the information was accessed through the shared system via a "viewer" that was built by hospital #3 to access OLIS information. It was the position of hospital #2 that hospital #3 had custody and control of the information that was accessed through the viewer because the information was contained in hospital #3's viewer. Given that hospital #3 had custody or control of the information, hospital #2 notified hospital #3 of the breach and also notified the affected patients.

Breach #3:

Hospital #3 received a complaint that a clerk had accessed her ex-spouse's personal health information without authorization. An investigation was initiated. The hospital did not suspend the clerk's access during the investigation because the clerk required access to complete her job duties. The hospital did advise the clerk that her accesses were being investigated and not to access the personal health information of the patient (her ex-spouse). The clerk went on leave during the course of the hospital's investigation.

The hospital's privacy office completed a further audit on the clerk's accesses. The audit identified access to the patient's file after the initial complaint and after the clerk was advised that her accesses were being investigated. The audit also identified 35 additional unauthorized accesses to six additional patients (family and colleagues). As part of the investigation, all affected patients were notified of the breach. The clerk was suspended from her duties and access to the system. The clerk was subsequently dismissed.

When asked about whether a lock-box was discussed with the patient and placed on the patient's file, hospital #3 advised that it could not feasibly place a block on the shared system to prevent the clerk from accessing a particular patient's records of personal health information. The hospital advised that Meditech has been unable to implement such a change to the system. The hospital advised that Meditech does have the ability to seal patient records from all users. The option of a lock-box was not discussed with the patient.

Hospital #3 advised that agents received privacy training upon hire but did not receive annual refresher training. Although agents were to have received training upon hire there was no record of training for the clerk involved in this breach.

The hospital advised that agents sign confidentiality agreements upon hire but hospital #3 did not require confidentiality agreements to be re-signed on an annual basis.

Hospital #3 completed random monthly audits as well as targeted audits.

Similar to hospital #1 and #2, there was no privacy notice on the shared system.

Breach #4:

An audit of two high profile patients of hospital #3 identified that an assistant of a customer of the shared system had accessed the personal health record of these two patients without authorization.

While an investigation was commenced, the assistant's access to the shared system was suspended and the assistant was also suspended from her job with pay. A further audit was completed. The further audit confirmed that the assistant had accessed the records of personal health information of 44 patients in the previous six months without authorization. The assistant was subsequently dismissed.

Hospital #3 notified the two high profile patients of the assistant's access. The remaining affected patients were not initially notified. Hospital #3 explained that there was confusion as to whether hospital #3 or the customer would complete the notification. This resulted in the additional patients not being notified at the time the breaches were identified. The remaining notifications occurred during the investigation by this office.

At the time of the breaches, hospital #3 advised that it relied on its customers to ensure their agents are aware of their privacy responsibilities through the customers' training protocols and confidentiality agreements.

The customers are not specifically required to train their agents or have them sign confidentiality agreements upon hire or annually. Hospital #3 advised that its customers are responsible for their own interpretation of the *Act*.

In this case, the assistant was provided training and signed a confidentiality agreement upon hire. The customer did not require its staff to complete annual privacy refresher training or the re-signing of confidentiality agreements.

Hospital #3 completed random monthly audits as well as targeted audits.

As noted above, there was no privacy notice on the shared system.

Breach #5:

The audit of the two high profile patients completed by hospital #3 in relation to breach #4 also identified that a laboratory staff member of a fourth hospital (hospital #4) had accessed the personal health information of one of the high profile patients through the shared system without authorization. In this case, hospital #4 managed the breach except for notification. Notification of the high profile patient was completed by hospital #3.

In response to the identified breach, hospital #4 completed a further audit covering the preceding 2-week period. The 2-week audit did not identify further breaches. Hospital #4 suspended the laboratory staff member without pay for five days and reported this agent to the relevant regulatory college.

At the time of the breach, this agent had received formal privacy training on one occasion and signed a confidentiality agreement on two occasions. Hospital #4 advised that it required its agents to complete annual privacy training. However, confidentiality agreements were not required to be signed on an annual basis.

With respect to audits, hospital #4 completed one random audit of a user's access and one random audit of access to a patient's record per month. This audit only covered the previous 2-week period. Hospital #4 explained that it is a smaller facility and one audit of a patient and a users' access each month was determined to be reasonable based on the service volume and number of agents. Hospital #4 also completed targeted audits.

As previously stated, the shared system did not have a privacy notice that agents viewed prior to accessing personal health information when this breach occurred.

Breach #6:

The above-mentioned audit of the high profile patients identified that a pharmacy staff member of hospital #3 had accessed one of the high profile patient's records of personal health information without authorization. The hospital commenced an investigation and a further audit was completed. The further audit identified additional unauthorized access to records of personal health information of five patients. Subsequently, the hospital determined that two of the accesses were not breaches.

The pharmacy staff member was notified about the investigation and advised not to go into patient records if it was not required by the pharmacy staff member's job duties.

As a result of the breaches, the pharmacy staff member received individual coaching and a disciplinary letter on file. A confidentiality agreement was also re-signed. In this case, the hospital was not able to locate the confidentiality agreement that the agent had originally signed.

The hospital notified the high profile patient of the breach. Three of the other affected patients were deceased and at the time of the breach, the hospital did not take any steps regarding notification. During the investigation by this office, hospital #3 subsequently placed a notification letter on the deceased patients' files and amended its process to include placing a notification letter on a patient's file if there is a breach and the patient is deceased or when a notification letter is returned due to a change in address.

Agents were not required to complete annual privacy training or re-sign confidentiality agreements annually. Privacy training and the signing of confidentiality agreements did occur upon hire.

The hospital completed targeted and monthly random audits. As noted in the other breaches, there was also no privacy notice viewed by agents prior to accessing personal health information on the shared system.

[24] The circumstances of the above breaches revealed some deficiencies in the hospitals' practices for protecting the privacy of the personal health information of their patients, in the context of their shared system. Among other things, auditing practices were inconsistent and training requirements insufficient. The hospitals failed to address how to respond to breaches of health information involving a provincial electronic

health record. Further, the hospitals had no policies or procedures enabling them to fulfill their lock-box obligations in the shared system.

SUMMARY OF THE INVESTIGATIONS OF THE SIX BREACHES:

[25] In conducting the investigation, I received submissions from each of the hospitals involved. In addition to the concerns identified above, the IPC asked for and reviewed various agreements and policies with respect to the status of hospital #3 as the HINP. As noted below, these agreements and policies raised further concerns regarding compliance with the obligations imposed on HINPs in the regulation to the *Act.*

[26] Each hospital confirmed that the accesses identified above were not authorized by the *Act*. In four of the identified breaches, the agents involved accessed personal health information that was not in the custody or control of the custodian on whose behalf the agent was acting. However, the agents were able to access the information through the shared system.

[27] In response to the breaches, the hospitals involved undertook to take a number of steps to address the IPC's concerns. Further, although these breaches only involved four hospitals from the group of custodians, the HINP/hospital #3 advised that all the custodians who signed the Agreement agreed to the steps taken to address the issues identified in the investigation. In addition, the customers are required to accept the policies, procedures and standards that are developed by the group of hospitals.

[28] In this decision, I accept the hospitals' conclusions that the collections, uses and disclosures of the personal health information at issue in these breaches were not authorized by the *Act.* I also find that the steps taken by the hospitals to protect personal health information insufficient in certain instances. Further, I find that the health information network provider did not comply with some provisions of section 6 of *Ontario Regulation 329/04.*

[29] However, in light of the steps taken by the group of custodians to address these issues, no review of this matter is warranted.

DISCUSSION

[30] There is no dispute that the hospitals involved in this investigation are "health information custodians" as defined in section 3(1) of the *Act*. There is further no dispute that hospital #3 is a health information network provider in relation to the shared system within the meaning of section 6 of *Ontario Regulation 329/04*.

[31] Additionally, there is no dispute that the records of personal health information accessed by the agents contain "personal health information" as defined in section 4(1)

of the *Act*.

ISSUES:

This decision addresses the following issues:

A. Was the personal health information "collected", "used" and "disclosed" in accordance with the *Act*?

B. Did the hospitals have and comply with information practices and take steps that were reasonable in the circumstances to protect personal health information in the shared system in accordance with the *Act*?

C. Did the HINP comply with section 6 of *Ontario Regulation 329/04*?

D. Is a review warranted under Part VI of the *Act*?

RESULTS OF INVESTIGATION:

Issue A: Was the personal health information "collected", "used" and "disclosed" in accordance with the *Act*?

[32] Section 2 of the *Act* defines "collect", "use" and "disclose" as follows:

> "collect", 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;
>
> "use", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to handle or 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.[7]
>
> "disclose", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information, and "disclosure" has a corresponding meaning;

[7] The definition of "use" was amended June 3, 2016; the change has no substantive impact on the outcome of this decision. I have quoted the provision in force prior to June 3, 2016 as it was in force at the time of the breaches.

[33] One of the purposes of the *Act* is to establish rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals, while facilitating the effective provision of health care.[8] One of the ways in which the *Act* achieves this purpose is by requiring that collections, uses and disclosures of personal health information occur with the consent of the individual to whom the information relates, except in limited cases.[9] The *Act* contains provisions relating to individuals providing express or implied consent to the collection, use or disclosure of their personal health information and, in certain circumstances, health information custodians can assume an individuals' implied consent to the collection, use or disclosure of their personal health information for health care purposes.[10]

[34] In addition to regulating custodians, the *Act* applies to the activities of those individuals who act for, or on behalf of, health information custodians in respect of personal health information. These individuals are referred to as "agents." Section 2 of the *Act* defines the terms "agent" as follows:

> "agent", in relation to a health information custodian, means 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 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;

[35] Section 6(1) clarifies that the provision of personal health information by a health information custodian to its agents is a "use" and not a "disclosure" under the *Act*:

> For the purposes of this *Act*, the providing of personal health information between a health information custodian and an agent of the custodian is a use by the custodian, and not a disclosure by the person providing the information or a collection by the person to whom the information is provided.

[36] Section 17 provides, among other things, that agents of a health information custodian may only collect, use, disclose, retain or dispose of personal health information in accordance with the *Act*.[11] It also provides that a health information custodian is responsible for any personal health information

---

[8] The *Act,* section 1(a).
[9] Ibid. section 29.
[10] Ibid. sections 18-20.
[11] Section 6 of *Ontario Regulation 329/04* made under the *Act* regulates non-agent electronic service providers as well was HINPs (whether an agent or not).

that is collected, used, disclosed, retained or disposed of by its agents.[12]

[37] As noted above, health information custodians participating in the shared system are considered to be the custodian of personal health information they created, contributed or collected. As such, where an agent of a custodian accesses personal health information that has been created, contributed, or collected by the custodian on whose behalf the agent is acting, this would be considered a "use". Conversely, when an agent accesses personal health information that was not created or contributed or collected by the custodian on whose behalf the agent is acting, that is a "collection" by the custodian on whose behalf the agent is acting and a "disclosure" by the custodian(s) with custody or control of the information.

[38] Ultimately, it does not matter whether the accesses by the agents in the above breaches are considered collections, uses or disclosures under the *Act* because, in any case, I accept that these accesses were unauthorized. No one suggested that any of the affected patients consented to the collection, use or disclosure of their personal health information nor that these collections, uses or disclosures were done for a health care purpose.[13] In fact, the hospitals at issue in these breaches reported that theses accesses were unauthorized. I have not been provided with information to suggest that these collections, uses or disclosures of personal health information would be authorized without consent under the *Act.*[14] As such, I accept that these collections, uses and disclosures were unauthorized.

Issue B: Did the hospitals have and comply with information practices and take steps that were reasonable in the circumstances to protect personal health information in the shared system in accordance with the *Act*?

[39] Section 10 of *the Act* states:

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.

2. A health information custodian shall comply with its information practices.

3. A health information custodian that uses electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any.

---

[12] Section 17 of the *Act* was amended June 3, 2016; the change has no substantive impact on this decision. I have quoted the provision in force prior to June 3, 2016 as it was in force at the time of the breaches.
[13] The *Act,* sections 18, 20(2) and 29.
[14] The *Act,* sections 36, 37, 38-48, 50

4. A person who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any.

[40] Section 2 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;

[41] Section 12(1) of the *Act* requires that health information custodians take "reasonable" steps to protect personal health information against unauthorized use or disclosure, among other things.[15] Specifically, section 12(1) of the *Act* states:

> 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.

[42] In Orders HO-010 and HO-013, and more recently in PHIPA Decisions 64 and 70, the IPC held that section 12(1) of the *Act* required health information custodians to review their measures or safeguards from time to time to ensure that they continue to be reasonable in the circumstances to protect personal health information in the custodians' custody or control. Health information custodians are expected to identify risks to privacy and take reasonable measures to reduce or eliminate such risks and mitigate the potential harms that may arise.

[43] Administrative and technical measures and safeguards are critical to protecting personal health information. The IPC has previously stated that, in order to comply with

---

[15] Section 11.1 of the *Act* imposes an obligation to protect against unauthorized collections. This section came into force on June 3, 2016 and was not in force at the time of the breaches. As a result, this section will not be addressed in this decision.

the requirement in section 12(1) of the *Act* to take steps that are reasonable in the circumstances to protect personal health information, custodians must implement administrative and technical measures or safeguards, including privacy policies, procedures and practices, audit functionality, as well as privacy training and awareness programs and initiatives.[16]

[44] Section 12(2) of the *Act* states the following:

> (2) Subject to subsection (3) 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.17

[45] Notably, this section requires health information custodians to notify individuals at the first reasonable opportunity when personal health information about that individual in the custodian's custody or control is stolen, lost, or accessed by unauthorized persons. There is no dispute that this section applies to the uses and disclosures at issue in the breaches.

[46] As part of my investigation, I examined the hospitals' privacy practices, against the obligations in sections 10, 12(1), and 12(2) of the *Act.* As noted briefly above, there were a number of inconsistencies and deficiencies in the policies and procedures of the hospitals participating in the shared system. Given my ultimate conclusion that the hospitals have adequately addressed the issues raised by these privacy breaches, it is unnecessary to make detailed determinations about whether these deficiencies amount to violations of the *Act*. I will explore the issues, concerns and the hospitals' responses in more detail below.

Administrative and Technical Measures and Safeguards:

Agreements:

[47] The HINP/hospital #3 advised that the original shared information service agreement applicable to the shared system was struck in 1999, prior to the enactment of the *Act* and section 6 of *Ontario Regulation 329/04* being brought into force. The original agreement included a schedule that set out terms and conditions relating to "health information". After the *Act* was enacted and *Ontario Regulation 329/04* was brought into force, an amending agreement was established that updated the relevant

---

[16] See HO-013.

[17] Section 12(2) of the *Act* was amended effective June 3, 2016; the change has no substantive impact on this decision. I have quoted the provision in force prior to June 3, 2016 as it was in force at the time of the breaches.

schedule in the Agreement to reflect some of the requirements of the *Act,* including defining personal health information, requiring compliance with some provisions of the *Act*, and addressing ownership of personal health information, privacy practices, confidentiality, security safeguards and the role of the steering committee.[18]

[48] However, the Agreement was not amended to specify the role of hospital #3 as the HINP in relation to the shared system or outline the requirements set out in section 6 of *Ontario Regulation 329/04*. The HINP/hospital #3, advised that although the amended Agreement did not refer to the HINP obligations in *Ontario Regulation 329/04*, it does provide a description of roles and responsibilities that the HINP/hospital #3 believed aligned with the *Act*.

[49] Previous orders of our office have noted that health information custodians should review their information practices and ensure that the information practices reflect any changes to operations, technologies and legislation.

[50] The need to keep abreast of these developments is particularly important in a shared system with multiple custodians and widely shared access. Any confusion about responsibilities could lead to significant consequences. In these circumstances, it is my view that the HINP and all health information custodians that are participating in a shared system should ensure that they have a written agreement and policies and procedures that reflect their respective legislated roles and responsibilities. This agreement and policies and procedures should reference the applicable roles and responsibilities imposed by the *Act* and its regulation and assign duties and obligations that comply with these requirements. In addition, should there be changes to privacy standards and best practices, amendments to the legislation/regulations or recommendations as a result of privacy and security audits, threat assessments or privacy impact assessments, etc., the agreement between the HINP and custodians participating in a shared system and their policies and procedures should be amended as necessary.

[51] The agreement governing the shared system at issue in this investigation did not reference or acknowledge hospital #3's role as the HINP for the shared system nor the specific obligations imposed on a HINP under Ontario law. While hospital #3 indicated its view that the roles and responsibilities set out in the agreement aligned with the *Act*, this is not a sufficient answer. Unless the agreement is explicit about the hospital #3's legal status as a HINP and the obligations that flow from that, the parties to the shared system will not have an adequate understanding of their respective roles and responsibilities in this relationship, and the statutory basis for them. This could in turn delay or impede responses to privacy breaches, changes in legislated duties, or other developments.

---

[18] I note that the Agreement was also amended other times in ways that are not relevant to this decision.

[52] As discussed in more detail below in relation to Issue C in this decision, when the IPC questioned hospital #3 regarding its compliance with section 6 of *Ontario Regulation 329/04*, it became clear that this hospital was not in full compliance with that section of the regulation. This demonstrates the need for clarity in the agreement about hospital #3's status as the HINP, and the obligations that flow from that.

[53] During this investigation, and in response to the IPC's concerns, the HINP and the custodians participating in the shared system added an appendix to the Agreement that outlined the HINP's obligations pursuant to *Ontario Regulation 329/04*.

Privacy Breach Management Policy:

[54] At the time of the breaches, the health information custodians with access to the shared system had developed a privacy breach management policy that applied to the shared system.

[55] The privacy breach management policy, that was to be followed by all health information custodians with access to the shared system, required the hospitals to follow their local policies for any breaches that did not affect another health information custodian. The system wide privacy breach management policy was to be followed when a privacy breach affected multiple custodians because the response would involve both the HINP and the affected custodians. The policy required the health information custodian or the HINP to advise the affected sites if a breach is detected. The policy notes that the site that detected the breach would likely take the lead on the investigation and that a conference call would be arranged to collectively plan an investigation and breach response, including containment and notification.

[56] The circumstances of the breaches at issue in this investigation revealed some shortcomings in the policy, which contributed to delays in notification of affected patients.

[57] As noted above, privacy breach #4 involved an assistant who worked for a customer of the shared system. The assistant had access to the personal health information of the custodians and customers participating in the shared system. Privacy breach #4 was discovered after an audit was completed on a high profile patient of hospital #3. Although there was a policy for the group of health information custodians participating in the shared system, the policy did not clearly indicate who was responsible for the notification of affected parties. A miscommunication between the hospital and the customer resulted in a failure to notify the additional affected parties of the breach at the first reasonable opportunity. During the course of this investigation, the additional affected parties were notified.

[58] In breach #6, no steps were taken by hospital #3 to address notification of the deceased patients. When an affected party is a deceased patient, custodians should notify the deceased's substitute decision maker where known. The timing and manner of notice may depend on the circumstances. If the deceased patient's substitute

decision maker is unknown a letter should be placed on the patients' file. During the investigation by this office, hospital #3 subsequently placed a notification letter on the deceased patients' files and amended its process to include placing a notification letter on a patient's file if there is a breach and the patient is deceased or when a notification letter is returned due to a change in address.

[59] In the case of privacy breach #2, the initial breach was identified from an OLIS report. Hospital #2's position was that the personal health information accessed through OLIS was in the custody or control of hospital #3 because the information was accessed through a viewer created by hospital #3. Thus, hospital #2 notified hospital #3 of the breach.

[60] OLIS is a province wide repository of laboratory tests and results. The IPC understands that the Ministry of Health (the ministry) has custody or control of the information contained in OLIS through their agent eHealth Ontario. The privacy breach management policy did not direct the custodians to notify eHealth or the ministry should there be a breach to the OLIS system. Further, the policy was also not clear on which custodian should have been responsible for notification of the ministry and/or eHealth Ontario in situations where the record accessed was through OLIS. The lack of guidance or communication regarding breaches that involve OLIS was troubling. An unauthorized access to the OLIS system should have been reported to the Ministry of Health through its agent eHealth Ontario as the custodian with custody or control of the information so that it could take appropriate steps.

[61] In addition to the above concerns about the shared system privacy breach management policy, there were some weaknesses in the hospitals' local privacy breach management policies. Hospital #1 did not have a privacy breach management policy outside of the policy available to the group of health information custodians of the shared system. Hospital #4's privacy breach management policy did not reference the specific steps the hospital was required to take as a custodian with access to the shared system and mistakenly identified the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) as the applicable legislation (as opposed to the *Act*).

[62] Custodians that are part of a shared system should all have consistent, comprehensive and legally accurate privacy breach management policies that include procedures addressing identification, reporting, containment, notification, investigation and remediation of suspected and actual privacy breaches. Privacy breach management policies must provide sufficient clarity so that health information custodians participating in a shared system are aware of what steps they are required to take and can be confident that patients who are entitled to be notified of a privacy breach involving their personal health information will, in fact, be notified.

[63] As described above, the shared system policy was not comprehensive and some of the hospitals' local privacy breach management policies were not consistent with the shared system policy, or were simply incorrect or non-existent.

[64] After I raised concerns regarding these policies and procedures, the working group agreed to take a number of steps regarding the privacy breach management policy for the shared system. The working group have reviewed their policies and procedures to ensure that all health information custodians with access to the shared system have consistent, comprehensive and legally accurate privacy breach management policies and procedures that address identification, reporting, containment, notification, investigation and remediation of all suspected and actual privacy breaches in the shared system.

[65] Of particular note, the custodians have revised their privacy breach management policies to clearly delineate which health information custodian is responsible for each step in the privacy breach management process. Further, hospital #2 has advised that any future breach of OLIS data would be governed by the Connecting Ontario policies and will require notice to the ministry.

Lock-box Policies and Procedures:

[66] Another issue that existed at the time of the breaches was with respect to lock-box policies and procedures. The term "lock-box" commonly refers to circumstances where an individual withholds or withdraws consent to the collection, use or disclosure of personal health information for a particular purpose, including for the provision of health care.[19] Under the *Act,* individuals can withhold or withdraw their consent to the collection, use or disclosure of their personal health information by health information custodians for health care purposes and may provide express instructions to health information custodians not to use or disclose their personal health information for health care purposes without consent.[20]

[67] Health information custodians are required to comply with the lock-box provisions of the *Act*.[21] Compliance with the lock-box provisions of the *Act* may be achieved through policies, procedures or manual processes, electronic or technological means or a combination of policies, procedures or manual processes and technological means.[22] While there may be functional limitations in the technology utilized by a health information custodian or group of health information custodians, this does not relieve them from their obligation to comply with the lock-box provisions of the *Act*. Where there are such technological limitations, health information custodians are required to explore other methods for ensuring that the lock-box provisions of the *Act* are complied with.

---

[19] Information and Privacy Commissioner/Ontario. (July 2005). *Lock-box Fact Sheet*. No. 8. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/fact-08-e.pdf
[20] Ibid; The *Act* sections 19, 20(2), 37(1)(a), 38(1)(a) and 50(1)(e)
[21] The *Act,* section 19, 20(2), 37(1)a, 38(1)a and 50(1)(e)
[22] Information and Privacy Commissioner/Ontario. (July 2005). *Lock-box Fact Sheet*. No. 8. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/fact-08-e.pdf

[68] In privacy breach #3, a patient raised a concern that his ex-spouse, a clerk at hospital #3, had accessed his personal health information. When the patient raised this concern, the privacy office and the clerk's manager discussed internally whether restrictions could be placed on the clerk's access. It was determined that a lock-box would not be implemented because the lock-box would place a broad restriction on the clerk's access which would restrict her from accessing the personal health information of other patients. Given that the clerk worked in the emergency department, it was determined that the clerk required access to other patients' personal health information in order to perform her job duties.

[69] Further, hospital #3 advised the IPC that, in order to restrict a single user from having access to a patients' file on the shared system, the hospital must manually input the user identification of all users with the exception of a single user, in this case the clerk, on each individual visit of the patient. The hospital advised that the effort to do this would be significant, therefore blocking access by a single user is not technically feasible in the shared system.

[70] As noted above, hospital #3 also advised the IPC that the shared system does have the ability to seal patient records from all users.

[71] Hospital #3 was plainly aware of the patient's privacy concerns. The hospital stated to the IPC that the patient did not request restrictions to his account and accepted the hospital's offer to monitor the clerk's accesses through the hospital's investigation process. The clerk subsequently accessed the patient's file, which was detected by the hospital during its investigation. The steps offered by the hospital did not prevent the clerk from accessing the patient's personal health information.

[72] In these particular circumstances, the IPC was concerned that the hospital apparently did not raise the possibility of a lock-box with the patient. While I understand that there are technical limitations at issue in the shared system preventing the hospital from specifically blocking this patient's record from the clerk, the hospital should have at least raised the lock-box provisions of the *Act* with the patient. The patient would then at least be in a position to effectively assert his rights and understand the options available to implement a lock-box. Further, the patient could have explored other options that may have been available in the shared system for flagging or restricting access to his record. As mentioned below, the hospital has now indicated it can create a flag that will pop-up when a particular patient's personal health information is accessed in the electronic management records module of the shared system.

[73] In addition to the above, in the course of this investigation the IPC learned that the custodians participating in the shared system did not have a system wide lock-box policy that addressed how to deal with the lack of a technological ability to restrict a users' access to a particular patient's personal health record. The lock-box policies that existed also did not address how the lock-box policy would be implemented across the shared system. This is a significant gap. When participating in a shared system, other

custodians accessing personal health information must be able to comply with patient lock-boxes through clear, comprehensive and system wide policies and procedures.

[74] The group of custodians and the HINP have committed to developing a new group wide policy and procedures that applies to "lock-boxes". This policy and procedures will include how a "lock-box" request is to be implemented in the shared system as well as, for each hospital, how the "lock-box" will be enforced and a requirement to discuss "lock-box" options with patients who have privacy concerns. The policy and procedures will also include options for how to implement a lock-box request given the functional limitations of the shared system. In preparing its updated system wide lock-box policy, the group has committed to having regard to the IPC's guidance document titled "Lock-box Fact Sheet".

[75] The group has also advised that it created a flag in the electronic management records module of the shared system. If implemented, when a particular patients' personal health information is accessed a box would pop-up. The pop-up box can be used to share information with the user.

Privacy Training and Education:

General Agent Training

[76] In *PHIPA* Decision HO-013, Commissioner Brian Beamish discussed the importance of privacy training in protecting personal health information:

> Comprehensive and frequent privacy training is essential to the development and maintenance of a culture of privacy within any organization. It is even more essential in an organization with custody or control of sensitive personal health information that is made widely available through electronic information systems.[23]

[77] Each hospital involved in this investigation responded to questions about its privacy training and education of its agents.

[78] At the time of the breaches, the hospitals provided privacy information (as distinguished from formal privacy training) to its agents throughout the year. This information was in various forms, such as relevant privacy information in newsletters, privacy information posted on department bulletin boards, discussion of relevant privacy issues at staff meetings, distribution of privacy pamphlets and consults and talks by the privacy office.

[79] Additionally, all hospitals provided training to their agents upon hire. However,

---

[23] HO-013, Page 34 and 36.

not all agents of the hospitals consistently received training prior to accessing personal health information or annually thereafter. At the time that the breaches took place, only hospital #4 provided its agents with privacy training on an annual basis. Hospital #2 did not provide its physician agents with any privacy training, either initially or thereafter.

[80] At the time of the breaches, the policies governing the hospitals collecting, using and disclosing personal health information by means of the shared system did not specifically require hospitals to provide any training to agents prior to initially granting access to personal health information in the shared system or thereafter. The HINP/hospital #3 advised that it relied on each custodian participating in the shared system to ensure that their agents were aware of their privacy responsibilities through their local training protocols. The HINP/hospital #3 considered training the responsibility of each custodian as the position of the HINP/hospital #3 was that each custodian was responsible for their own interpretation of the *Act*.

[81] In my view, where health information custodians are pooling their personal health information in a shared system, it is untenable for each custodian to be responsible for their own interpretation of the *Act*. Where one custodian is granting access to a system containing personal health information in its custody or control to an agent of another custodian, that agent must be instructed on the terms under which access is granted (including conditions and restrictions on access). Without consistent and comprehensive training across all health information custodians with access to the shared system, there can be confusion among the agents of the various health information custodians as to what is, and is not, permitted in the shared system. Additionally, without consistent and comprehensive training policies, the health information custodians that are participating in the shared system are granting other health information custodians' agents access to personal health information in their custody or control in the absence of steps to ensure those agents of other custodians understand what they are permitted to do with the accessible personal health information.

[82] In the case of this group of custodians, there were no written policies and procedures that established clear minimum training standards for the shared system.

[83] In response to the IPC's concerns, the working group established by the group of custodians have established minimum training standards across the shared system. The training standards include minimum requirements that privacy training be provided to everyone accessing personal health information on the shared system prior to gaining access to the system and that privacy training be completed on an annual basis thereafter. When establishing its training standards, the group will have regard to our office's guidance document titled "Detecting and Deterring Unauthorized Access to Personal Health Information".

[84] All health information custodians of the shared system are now required to have all agents, including their physicians, receive initial and annual privacy training and track the training.

Privacy Officer Training

[85] During the investigation of the reported breaches, it became clear that the information displayed on the audit reports conducted by the hospitals varied. Hospital #1's audit report did not display the length of time the user accessed the various screens of a patient's personal health record in the shared system. The other hospitals in this investigation were able to produce audit reports that included this information.

[86] In the shared system, the auditing function included the ability for an audit report to include the length of time that an agent accessed a particular screen of personal health information. This function could assist custodians to determine whether an agent's access to a personal health record was unauthorized or not. Hospital #1 was unaware of this function. All privacy officers with access to the same shared system should have the same tools when monitoring agents for unauthorized access and know how to effectively use the available auditing systems.

[87] As a result of this investigation, the health information custodians developed and implemented training for their privacy officers on Meditech's auditing capabilities so that privacy officers across the shared system are aware of all of the relevant features and capabilities.

Confidentiality Agreements:

[88] Each hospital involved in this investigation responded to questions about the signing of confidentiality agreements.

[89] All the hospitals involved had their agents' sign a confidentiality agreement at the time of hire. However, only hospital #4 consistently had agents re-sign confidentiality agreements annually and tracked the signing of confidentiality agreements. The re-signing and tracking at the other hospitals involved was inconsistent or nonexistent. For instance, hospital #2 had agents re-sign the confidentiality agreements at performance reviews but performance reviews were not consistently being completed on an annual basis. This resulted in confidentiality agreements not being signed annually.

[90] At hospital #3, agents were not required to re-sign confidentiality agreements. The confidentiality agreements were only re-signed when warranted such as when there was a privacy incident. In addition, in breach #6, hospital #3 advised that the pharmacy staff member had signed a confidentiality agreement but hospital #3 was unable to locate a copy of the signed confidentiality agreement.

[91] Requiring agents to sign confidentiality agreements on a regular basis may help to prevent or reduce the risk of unauthorized access to personal health information.

Confidentiality agreements require agents to acknowledge privacy obligations and expectations, including the consequences of a privacy breach.[24]

[92] The group of custodians had no written document that established minimum standards regarding confidentiality agreements across the shared system. The hospitals did require their agents to sign confidentiality agreements upon hire, but hospitals #1, #2 and #3 did not require all agents to re-sign confidentiality agreements on an annual basis or track the signing of confidentiality agreements.

[93] I raised concerns with the hospitals about the inconsistencies and gaps in their practices with respect to confidentiality agreements. During the course of this investigation all hospitals involved have advised that their agents now re-sign confidentiality agreements on an annual basis. In addition, the working group have also agreed to establish minimum standards across the shared system applicable to confidentiality agreements. The minimum standards will include that confidentiality agreements are to be signed prior to gaining access to the shared system and annually thereafter. Finally, the hospitals also now track the signing of confidentiality agreements.

Privacy Notice:

[94] Privacy notices remind custodians and their agents of their obligations and of the consequences of unauthorized access and may also serve to prevent or reduce the risk of unauthorized access to personal health information.[25]

[95] At the time of the breaches, the shared system did not have a privacy notice that agents accessing the shared system would view prior to accessing personal health information. During the course of the IPC's investigation, a privacy notice was implemented on the shared system as of March 2016.

[96] The agents at all health information custodians with access to the shared system now view two notices. The first notice is viewed when an agent initially logs in to the shared system. The first notice advises agents that access to personal health information is tracked daily and audited regularly. Agents are advised that they are only allowed to view personal health information to provide direct patient care or when needed to perform assigned duties. Agents are also warned that failure to comply could

---

[24] Information and Privacy Commissioner of Ontario. Detecting and Deterring Unauthorized Access to Personal Health Information. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/detect_deter.pdf

[25] Information and Privacy Commissioner of Ontario. (January 2015) *Detecting and Deterring Unauthorized Access to Personal Health Information*. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/detect_deter.pdf
See also IPC orders HO-010 and HO-013.

result in disciplinary action up to termination as well as fines may be imposed on the user.

[97] A second notice is viewed when an agent accesses a record in the shared system that was created by another custodian. The second notice informs the agent that the personal health record the agent is accessing contains records of personal health information from visits to another health information custodian with access to the shared system. The agents then have the opportunity to select to access the additional records from visits at another health information custodian in the shared system, or not. The agents are advised that the access is recorded in the shared system.

Auditing:

[98] In *PHIPA* Order HO-013, Commissioner Brian Beamish described the role of auditing in protecting personal health information:

> Auditing of electronic information systems is particularly important in ensuring that the privacy of individuals and the confidentiality of personal health information are protected. Audits are essential technical safeguards for electronic information systems. They can be used to deter and detect collections, uses and disclosures of personal health information and the copying, modification or disposal of records of personal health information that contravene the *Act* . As such, they help to maintain the integrity and confidentiality of personal health information stored in electronic information systems. The ability to conduct audits of personal health information and the activities of agents or users (referred to in this section as users) in an electronic information system also ensures that a health information custodian is able to respond to requests from patients for information about who has collected, used or disclosed their personal health information.
>
> In order to be effective, audits require analyzable data about the full extent to which users collected, used, disclosed, copied, modified or disposed of personal health information within a given time period. If such data is not available or is only available in part, then a health information custodian will not be able to conduct a complete audit in relation to the personal health information stored in its electronic information system.[26]

[99] At the time of the breaches, the group of custodians participating in the shared system had implemented auditing policies for each health information custodian with access to the shared system to follow. The auditing policy for the group of custodians

---

[26] HO-013, page 23.

required the health information custodians to complete random audits on a monthly basis for the previous month. The policy also required health information custodians to complete targeted audits if unauthorized access is suspected. The policy outlined that if activity identified by the audit involves another health information custodian in the shared system, the hospitals were to engage that custodian as necessary and agree on who would communicate with the patient or user as necessary.

[100] All the hospitals involved advised that random and targeted audits were completed, however, the frequency of audits and length of period audited were not consistent. For example, hospital#4 advised that the functionality of the user audit log within Meditech only permitted auditing of two weeks of historical information which did not comply with the shared system auditing policy. Interestingly, the other hospitals involved in this investigation reported that they were able to complete longer audits on their users' accesses to the shared system.

[101] Hospital #2 advised that there was a vacancy in the privacy office and, as a result, for a period of approximately a year and four months, the hospital only completed audits on a quarterly basis. The auditing practices of hospital #2 for this time period did not comply with the auditing policy of the shared system which stated that audits were to be completed on a monthly basis.

[102] Finally, the information that displayed on the audit reports conducted by the hospitals varied. For example, hospital #1's audit report did not display the length of time the user accessed the various screens in the shared system and, as discussed above, the privacy officer was unaware of how to run a report displaying this information. The other hospitals in this investigation were able to produce audit reports that included this information.

[103] The above facts demonstrated deficiencies and inconsistencies in the hospitals' collective auditing practices. In response, the working group have agreed to establish a minimum standard of auditing capability. The minimum standard for auditing will include a standard for the type of data displayed and a minimum standard retention period that is significantly longer than 2 weeks.

[104] In addition, hospital #2 has confirmed that the vacancy in its privacy office was filled and audits are now completed on a monthly basis. In response to contact with our office during this investigation, hospital #1 consulted with the other hospitals in the shared system and was able to incorporate the length of time an agent accesses a particular screen in audit reports moving forward.

[105] As noted above, as a result of this investigation, the health information custodians developed and implemented training for their privacy officers on Meditech's auditing capabilities so that privacy officers of health information custodians with access to the shared system are aware of all of the features and capabilities of the system.

Issue C: Did the HINP comply with section 6 of *Ontario Regulation 329/04?*

[106] Section 6 of *Ontario Regulation 329/04* (the Regulation) sets out a number of requirements for HINPs. Section 6 specifically states the following:

> 6. (1) Except as otherwise required by law, the following are prescribed as requirements for the purposes of subsection 10 (4) of the Act with respect to a person who supplies services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, and who is not an agent of the custodian:
>
> > 1. The person shall not use any personal health information to which it has access in the course of providing the services for the health information custodian except as necessary in the course of providing the services.
> >
> > 2. The person shall not disclose any personal health information to which it has access in the course of providing the services for the health information custodian.
> >
> > 3. The person shall not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the person who is subject to this subsection.
>
> (2) In subsection (3),
>
> > "health information network provider" or "provider" means a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians. O. Reg. 329/04, s. 6 (2).
>
> (3) The following are prescribed as requirements with respect to a health information network provider in the course of providing services to enable a health information custodian to use electronic means to collect, use, disclose, retain or dispose of personal health information:
>
> > 1. The provider shall notify every applicable health information custodian at the first reasonable opportunity if,

i. the provider accessed, used, disclosed or disposed of personal health information other than in accordance with paragraphs 1 and 2 of subsection (1), or

ii. an unauthorized person accessed the personal health information.

2. The provider shall provide to each applicable health information custodian a plain language description of the services that the provider provides to the custodians, that is appropriate for sharing with the individuals to whom the personal health information relates, including a general description of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information.

3. The provider shall make available to the public,

i. the description referred to in paragraph 2,

ii. any directives, guidelines and policies of the provider that apply to the services that the provider provides to the health information custodians to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information, and

iii. a general description of the safeguards implemented by the person in relation to the security and confidentiality of the information.

4. The provider shall to the extent reasonably practical, and in a manner that is reasonably practical, keep and make available to each applicable health information custodian, on the request of the custodian, an electronic record of,

i. all accesses to all or part of the personal health information associated with the custodian being held in equipment controlled by the provider, which record shall identify the person who accessed the information and the date and time of the access, and

ii. all transfers of all or part of the information associated with the custodian by means of equipment controlled by the provider, which record shall identify the person who transferred the information and the person or address to whom it was sent, and the date and time it was sent.

5. The provider shall perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to,

i. threats, vulnerabilities and risks to the security and integrity of the personal health information, and

ii. how the services may affect the privacy of the individuals who are the subject of the information.

6. The provider shall ensure that any third party it retains to assist in providing services to a health information custodian agrees to comply with the restrictions and conditions that are necessary to enable the provider to comply with this section.

7. The provider shall enter into a written agreement with each health information custodian concerning the services provided to the custodian that,

i. describes the services that the provider is required to provide for the custodian,

ii. describes the administrative, technical and physical safeguards relating to the confidentiality and security of the information, and

iii. requires the provider to comply with the Act and the regulations.

(4) A health information custodian who uses goods or services supplied by a person referred to in subsection 10 (4) of the Act, other than a person who is an agent of the custodian, for the purpose of using electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall not be considered in so doing to make the information available or to release it to that person for the purposes of the definition of "disclose" in section 2 of the Act if,

(a) the person complies with subsections (1) and (3), to the extent that either is applicable, in supplying services; and

(b) in the case of a person supplying goods to the health information custodian, the custodian does not, in returning the goods to the person, enable the person to access the personal health information except where subsection (1) applies and is complied with.

[107] Where a HINP is not an agent of the health information custodian to whom it is providing the services mentioned in section 6(2), the HINP must comply with the obligations imposed by section 6(1) of the Regulation [in addition to the obligations imposed by s. 6(3)]. Where a HINP is an agent of the health information custodian to whom it is providing the services mentioned in 6(2), it must comply with section 17 of the *Act* (in addition to the obligations imposed by s. 6(3)).

[108] The HINP and the hospitals involved with this investigation were asked to provide any agreements or documents they had to show compliance with the requirements set out in section 6 of the Regulation. They provided a copy of shared system and hospital policies as well as the Agreement (including various amending agreements) between the HINP and the hospitals.

[109] As discussed above, it was clear that the Agreement governing the shared system did not reference or acknowledge hospital #3's role as the HINP for the shared system nor the specific obligations imposed on a HINP under Ontario law, and there was no document provided to the IPC that did so.

[110] Further, there was no agreement that would comply with all of the requirements of paragraph 7 of section 6(3) of the Regulation. Paragraph 7 of section 6(3) of the Regulation requires that the HINP enter a written agreement with each custodian that describes the services that the provider is required to provide the custodian, describes the administrative, technical and physical safeguards relating to the confidentiality and security of the information, and requires the provider to comply with the *Act* and the regulations.

[111] The health information custodians with access to the shared system did not have such an agreement with the HINP. Specifically, the existing agreement failed to describe the administrative, technical and physical safeguards relating to the confidentiality and security of the information.

[112] Paragraph 2 of section 6(3) requires that the HINP provide to each custodian a plain language description of the services it provides. The HINP advised that it only provided such a plain language description upon request.

[113] Finally, paragraph 3 of section 6(3) of the Regulation requires that the HINP make certain information available to the public. This information comprises the plain language description referred in paragraph 2 of section 6(3), any directives, guidelines and policies that apply to the services that the HINP provides to the custodians (with exceptions) and a general description of the safeguards implemented by the HINP in relation to the security and confidentiality of the information. At the time of the breaches, the HINP had not made the above noted information available to the public.

[114] Based on the information provided, at the time of the breaches the HINP had not taken all the required steps to comply with section 6 of the Regulation. In order to address these concerns and become compliant with the requirements of the Regulation,

the HINP agreed to take a number of steps, including revising its Agreement to comply with paragraph 7 of section 6(3). I also note, as indicated above, that during this investigation, the HINP and custodians participating in the shared system, added an appendix to the Agreement that outlined the HINP's obligations pursuant to *Ontario Regulation 329/04*.

[115] The HINP has also agreed to revise its external webpage to provide information to the public in accordance with paragraph 3 of section 6(3) of the Regulation and provide each applicable health information custodian with the information set out in paragraph 2 of section 6(3) of the Regulation. The HINP has made this information available on its website.

[116] In light of the steps taken by the HINP to address the shortfalls in complying with section 6 of the Regulation, I am satisfied it has since addressed the issues or committed to addressing the issues.

Issue D: Is a review warranted under Part VI of the *Act*?

[117] Section 58(1) of the *Act* sets out the Commissioner's discretionary authority to conduct a review as follows:

> The Commissioner may, on his or her own initiative, conduct a review of any matter if the Commissioner has reasonable grounds to believe that a person has contravened or is about to contravene a provision of this Act or its regulations and that the subject-matter of the review relates to the contravention.

[118] While I have found deficiencies in the privacy practices of the hospitals in this shared system, these issues have been addressed as set out above. In accordance with my delegated authority to determine whether a review is conducted under section 58(1) of the *Act* and for the reasons set out above, I find that a review is not warranted.

NO REVIEW:

1. For the foregoing reasons, no review of this matter will be conducted under Part VI of the *Act.*

Original signed by
Alanna Maloney
PHIPA Investigator

October 30, 2019