

PHIPA Order

H0-013

December 16, 2014

EXECUTIVE SUMMARY

Personal health information is considered to be among the most sensitive types of personal information, deserving of the highest protection. Yet, in Ontario, we have seen a growing number of cases of agents inappropriately accessing the personal health information of individuals. The type and magnitude of these violations vary. Some involve celebrity “gawkers,” others nosy neighbours, family members or work colleagues. The circumstances of this case involve the unauthorized use and disclosure of personal health information for financial gain. The message to take from all of these cases is clear. Authorized users of electronic information systems can abuse their access privileges — they pose a risk to patient privacy. Health information custodians must implement reasonable measures and safeguards to eliminate or reduce these risks and to mitigate the harms that may arise from them.

Within the span of less than a year, the Rouge Valley Health System (the Hospital) reported two separate breaches of patient privacy to the Office of the Information and Privacy Commissioner of Ontario. The first reported breach was received by this office in September 2013 and the second, seven months later, in April 2014. Although separate incidents, the breaches were materially similar in that both involved allegations that Hospital employees in clerical positions used and/or disclosed the personal health information of mothers who had recently given birth at the Hospital for the purposes of selling or marketing Registered Education Savings Plans (RESPs).

Given the pattern that appeared to be emerging, upon notification of the second breach, this office decided to conduct a review under the *Personal Health Information Protection Act, 2004* (the *Act*). During this review, we conducted extensive interviews. We engaged in a thorough review of the Hospital’s relevant policies, practices and procedures and received written representations from the Hospital.

As a consequence of the two reported breaches, the Hospital notified more than 14,000 current and former patients of its Rouge Valley Centenary site and Rouge Valley Ajax and Pickering site, all of whom *may* have been affected by the actions of the two employees. It was necessary to notify all of these individuals because the Hospital was unable to identify the individuals who were actually affected by the actions of the two employees involved in the reported breaches.

Following the first breach, the Hospital discovered that the audit functionality of its Meditech system, the electronic information system at issue in this review, was limited and it undertook to address this shortcoming. During this review, we learned that despite the actions taken and the similarity between the two breaches, the Hospital was still unable to conduct an audit of user activities relating to the second breach due to another “gap” in the Meditech system’s audit functionality.

Audits are essential technical safeguards to protect personal health information. They can be used to deter and detect collections, uses and disclosures of personal health information that contravene the *Act*. In this way, they help to maintain the integrity and confidentiality of personal health information stored in electronic information systems. The Hospital's failure to implement full audit functionality in its Meditech system meant that it could not comply with its own policies and that it did not comply with the requirements of the *Act*.

We also learned that the Hospital's administrative measures or safeguards such as privacy policies, procedures and practices as well as privacy training and awareness programs — which are critical in protecting personal health information — were insufficient and therefore not in compliance with the *Act*. These types of safeguards are particularly important in relation to electronic information systems which provide agents with the ability to access a vast amount of personal health information.

In this Order, among other things, I find that the Hospital failed to comply with its obligations under the *Act* to put in place technical and administrative measures or safeguards to protect personal health information in compliance with section 12(1) of the *Act* and I order the Hospital to:

1. In relation to all of the Hospital's electronic information systems, implement the measures necessary to ensure that the Hospital is able to audit all instances where agents access personal health information on its electronic information systems, including the selection of patient names on the patient index of its Meditech system.
2. In relation to the Hospital's Meditech system:
 - a) Work with the Hospital's Hosting Provider to review and amend the service level agreement between the Hospital and the Hosting Provider to clarify the responsibility for the creation, maintenance and archiving of user activity logs generated by the Hospital's use of its Meditech system, and ensure that the user activity logs are available to the Hospital for audit purposes.
 - b) Work with Meditech or another software provider to develop a solution that will limit the search capabilities and search functionalities of the Hospital's Meditech system so that agents are unable to perform open-ended searches for personal health information about individuals, including newborns and/or their mothers, and can only perform searches based on the following criteria: health number, medical record number, encounter number, or exact first name, last name and date of birth.
3. Review and revise its *Privacy Audits* policy, the *Pledge of Confidentiality* policy and the "Pledge of Confidentiality," and the *Privacy Advisory* in accordance with the comments and findings made in this Order, and take steps to ensure that it complies with the *Privacy Audits* policy.
4. Develop and implement a *Privacy Training Program* policy, a *Privacy Awareness Program*

policy, and a *Privacy Breach Management* policy in accordance with the comments and findings made in this Order.

5. **Immediately** review and revise its privacy training tools and materials in accordance with the comments and findings made in this Order.
6. Using the privacy training materials developed in accordance with Order provision 5:
 - a) **immediately** conduct privacy training for all agents in clerical positions in the Hospital; and
 - b) conduct privacy training for all other agents by **June 16, 2015**.
7. Provide this office with proof of compliance with all of the Order provisions by **September 16, 2015**.

BACKGROUND

Within the span of less than a year, the Rouge Valley Health System (the Hospital) reported two separate breaches to the Office of the Information and Privacy Commissioner of Ontario (IPC). The first breach was reported to the IPC in September 2013 and the second, seven months later, in April 2014. Although the reported breaches involved separate incidents, they were materially similar in that both involved allegations that Hospital employees in clerical positions used and/or disclosed the personal health information of mothers who had recently given birth at the Hospital for the purposes of selling or marketing Registered Education Savings Plans (RESPs). Given the pattern that appeared to be emerging, upon receipt of the report of the second breach, the IPC decided to conduct a review pursuant to section 58(1) of the *Personal Health Information Protection Act, 2004* (the *Act*).

The circumstances surrounding the two reported breaches are complex. Before going into the details of the two breaches, it is necessary to provide some background on the Hospital as well as on the electronic information system at issue in this review.

The Hospital

The Hospital operates two community hospital sites, Rouge Valley Centenary (Centenary site) and Rouge Valley Ajax and Pickering (Ajax and Pickering site). The Centenary site is located in east Toronto and the Ajax and Pickering site is located in west Durham. The two employees who were the subject of the reported breaches were employed at the Centenary site, but had access to the personal health information of patients at both sites through one of the Hospital's electronic information systems.

Electronic Information System

The Hospital uses electronic information systems to facilitate the provision of health care to its patients. While the Hospital maintains records of personal health information in paper format, there has been nothing to suggest that the two employees who were the subject of the reported breaches used and/or disclosed personal health information in paper form for the purposes of selling or marketing RESPs.

The software that runs the electronic information system at issue is named after the company that provides it. That company is Medical Information Technology, Inc. (Meditech). In this Order, I will use “Meditech” to refer to the company and “Meditech system” to refer to the electronic information system at issue. The information that the IPC received about the Hospital’s Meditech system was provided by the Hospital in its representations filed during this review.

The Hospital’s Meditech system is a collection of different applications called “modules.” Different modules assist employees and other agents of the Hospital in performing different high-level tasks; for example, scheduling, admissions, payroll, billing, etc. At a lower level than modules are components of modules. Components of modules perform specific functions. For example, the patient index is a component that is present in the scheduling module. The patient index, an electronic list of every Hospital patient, allows employees and other agents of the Hospital with access to it to search for patients in the Hospital’s database.

The scheduling module was used by the two employees to access the personal health information of new mothers. The employees were granted access to this module to perform their duties, which included registering patients and scheduling appointments and procedures for them. The first step in scheduling an appointment or procedure is to determine whether the person is an existing Hospital patient by searching for their name on the patient index. If the patient is not on the patient index, then they must be registered and issued a medical record number (MRN). This two-step task requires access to the *entire* patient index so as to prevent the same patient from being registered multiple times and receiving multiple MRNs. For this reason, the two employees had access to the personal health information of patients at both the Hospital’s Centenary site and Ajax and Pickering site, including demographic information about patients, such as their name, address and phone numbers, date of birth, health number and the dates of visits to the Hospital.

The Hospital shares a version of Meditech software with another hospital that runs the software and hosts the Meditech system used by the Hospital. In this Order, this other hospital will be referred to as the “Hosting Provider.” The Hosting Provider owns the license for the shared Meditech software and is responsible for implementing and operating a Meditech system on behalf of the Hospital according to a service level agreement between them. A consequence of the fact that the Hospital and Hosting Provider share a version of Meditech software is that some technical settings apply to both the Hospital and the Hosting Provider.

Clerical Staff

As noted above, the responsibilities of the two employees who were the subject of the reported breaches included performing tasks such as registering patients, and scheduling appointments and procedures for them. However, the two employees' responsibilities were not limited to such tasks. Throughout this Order, those who work in positions with similar responsibilities as the two employees will be referred to generally as "clerical staff." Clerical staff are not responsible for directly providing health care to patients.

Reported Breach 1

In September 2013, the Hospital contacted the IPC to report a breach involving an employee (Employee 1) who it determined had violated the Hospital's privacy policy and the *Act*. Employee 1 began working in a clerical position at the Centenary site in May 2004. In July 2013, Employee 1 was transferred to another department at the Centenary site, where he continued to work in a clerical position until he was terminated in October 2013.

In 2009, Employee 1 advised the Hospital that he had applied for a part-time position as a sales representative for an RESP company and he asked the Hospital to confirm, in writing, that selling RESPs would not be a conflict of interest vis-à-vis his employment with the Hospital. In July 2009, the Hospital provided Employee 1 with a letter, which stated:

It is our understanding that one of our employees, [name of Employee 1] has applied for an RESP sales representative position. Many of our staff hold jobs apart from working here and all employees who hold other positions outside of their employment with Rouge Valley Health System must abide by our rules and regulations, including our Conflict of Interest Policy, which states, in part, that no employee shall solicit any business from patients, staff or visitors to support such outside employment.

When Employee 1 was transferred in July 2013, his access to Meditech system modules that included personal health information was terminated, because the Hospital determined that he no longer required that access to fulfil his job duties. According to the Hospital, shortly after his transfer, Employee 1 asked the Hospital to reinstate his access to Meditech system modules that included personal health information, stating, at that time, that he was "seeking access to phone numbers of patients who had recently given birth in order to sell them RESPs in the course of his part-time employment." Based on this information, Employee 1 was suspended pending the outcome of an investigation by the Hospital. His access to personal health information was also suspended.

The Hospital advised that during a subsequent interview by its human resources staff, Employee 1 denied that he was employed part-time selling RESPs or that he had contacted any patients of the Hospital for that purpose. Shortly after that interview, the Hospital terminated

Employee 1 having concluded that he had violated the Hospital's privacy policy and the *Act*.

During discussions we had with Employee 1, he continued to deny that he had contravened the Hospital's policies and the *Act*. However, given the Hospital's findings and the fact that it reported a privacy breach to this office, for the purposes of this Order, I accept the Hospital's conclusion that Employee 1 had contravened its policies and the *Act*.

When this breach was reported to the IPC in September 2013, the IPC believed that it was an isolated incident and, based on the information provided by the Hospital as to the steps that it had taken or would take to minimize the risk of a similar breach occurring in future, the IPC worked with the Hospital to contain the breach and to ensure that appropriate notice to affected patients was given. Further discussion of the Hospital's response to this reported breach appears below.

In a letter dated October 8, 2013, the Hospital provided the IPC with the results of its internal investigation, including the following information:

The Hospital "determined that the incident was a violation of the [Hospital] privacy policy and the PHIPA act, and self-reported the incident to the IPC."

The Hospital's IT department was not able to prove or disprove that Employee 1 had been "accessing patient records" because the Hospital's "system only has two weeks of user history" which was "a limitation posed by [its] Meditech hosting partner."

The Hospital "[e]stablished that the employee had access to schedule information which allowed him to view contact information (telephone and address) of expecting mothers without accessing the patient record."

The Hospital was not "able to view patient record level audit logs" and therefore was also "not able to quantify the number of patients whose information was viewed inappropriately by the employee."

With respect to the limitations of its audit functionality, the Hospital stated:

In order to overcome the audit log limitation that we discovered in our Meditech system, we are working with our hosting party, [], and the vendor, Meditech, on two enhancements of the access logs: (a) extend the length of the live Meditech log to ninety days and enable the archiving of the logs past ninety days, (b) create an export of the access logs from the Meditech proprietary format to a relational database that will allow us to maintain unlimited access history and report inappropriate access.

On December 12, 2013, the Hospital began notifying 7,613 current and former patients that their personal health information may have been used by Employee 1 in contravention of the *Act*. Not knowing for certain which patients' personal health information was used by Employee 1, the Hospital notified all patients at the Centenary site who had given birth between July 2009

and August 2013, which is the period of Employee 1's employment for which he had access to the scheduling module of the Meditech system.

Reported Breach 2

On April 24, 2014, the Hospital notified the IPC that it had discovered that a second employee (Employee 2) had been selling the personal health information of patients who had recently given birth at the Hospital to an RESP company.

Employee 2 began working in a clerical position at the Hospital's Centenary site in July 2001 and continued to work in that capacity until June 2013. In July 2013, Employee 2 began working again in a clerical position at the Hospital's Centenary site until her resignation in April 2014.

The Hospital explained that in early April 2014, one of its staff members found a number of documents on a printer that appeared to be printed screen shots of the Meditech system. The Hospital stated that the documents included the personal health information of patients who had recently given birth. The screen shots were given to senior managers, who determined that Employee 2 had printed them.

In representations submitted by the Hospital during this review, the Hospital states that the printed screen shots represented the results of searches conducted on the patient index. The results included a "lookup list of patients meeting the search parameters" used by Employee 2. In addition, the printed screen shots included the patient "selected" from the list which pulls up the patient's contact information, health number and Hospital visits. These search results indicated that Employee 2 was looking for information about new mothers.

The Hospital conducted an internal investigation. During this internal investigation, Employee 2 admitted to the Hospital that she had been selling personal health information to an RESP sales agent since 2010 and stated that she had sold the information of about 400 patients in the last nine months of her employment for approximately \$600. After the Hospital concluded its internal investigation in April 2014, Employee 2 resigned.

On May 27, 2014, the Hospital notified an additional 669 former patients of its Centenary site that "a staff member was inappropriately accessing hospital information through the Hospital's electronic scheduling system." This group of patients was comprised of the mothers who had given birth at the Hospital's Centenary site between July 2013 and April 2014 — the period of time between the first reported breach and the second reported breach. The Hospital states in its representations that it was not able to identify the actual patients affected by Employee 2's actions.

Further Notification to Patients

On July 2, 2014, the Hospital informed the IPC that the screen shots that were found on the printer that triggered its investigation into the activities of Employee 2, contained the personal health information of patients who had received care at its Ajax and Pickering site, in addition to its Centenary site. In light of this and given that Employee 1 also had access to the Meditech patient index, which includes the personal health information of patients at the Ajax and Pickering site, the Hospital concluded that some patients at the Ajax and Pickering site may have been affected by the activities of the two Employees.

On August 19, 2014, the Hospital notified a further 6,150 former patients of the Ajax and Pickering site that their personal health information may have been used and/or disclosed in contravention of the *Act*.

REVIEW PROCESS

Following the report of the second breach, the IPC commenced a review under section 58(1) of the *Act* and began to gather further information from the Hospital including copies of relevant documents, such as copies of the applicable policies, practices and procedures of the Hospital.

The IPC also met with and interviewed the Chief Information and Privacy Officer and other senior managers at the Hospital, and was given a demonstration of the Meditech system and its scheduling module that was used by both Employees in the regular course of their employment. Hospital IT staff also gave a demonstration of the audit capabilities and limitations of the Meditech system.

The IPC contacted both Employees and asked them to meet with IPC staff. Employee 1 declined, but Employee 2 agreed to be interviewed.

Given the seriousness of the allegations, I issued a summons to both Employees pursuant to section 60(12) of the *Act*. The summons compelled them to attend at the office of the IPC and to give evidence under oath or affirmation.

I also issued a Notice of Review asking the Hospital to submit written representations on the issues relevant to this review. After receipt of representations in response to the initial Notice of Review, I issued a Supplementary Notice of Review inviting the Hospital to submit further representations. I received representations from the Hospital in response to the supplementary notice.

Other Hospitals

During the course of this review, the IPC received complaints from 20 different individuals who

had given birth at other Ontario hospitals and who had been contacted by telephone in the days or weeks following their child's birth by representatives of various RESP companies ("complainants").

Seventeen of these complainants provided their consent to an investigation by this office into the circumstances surrounding their complaint. The IPC then contacted the hospitals identified and requested that they conduct their own internal investigations and report back to the IPC on the results of those investigations. The hospitals' internal investigations included audits of the personal health information of the complainants and, in some cases, the hospitals contacted the RESP companies involved to inquire as to how the RESP company received the contact details of the complainants. The IPC received the full cooperation of the hospitals involved.

I am satisfied that in each of these cases involving other hospitals, the personal health information of the complainants was not used and/or disclosed by agents of the other hospitals for the purposes of selling or marketing RESPs. Based on the reports received from the other hospitals, the IPC learned that the complainants had, at some point prior to the birth of their child, provided their consent to be contacted by an RESP company. This consent was provided in some cases on ballot entries submitted at baby shows or exhibitions, and/or by signing up for a loyalty card at a maternity clothing retailer. Most of these complainants did not recall providing their consent and acknowledged that they might not have thoroughly reviewed the information on the ballot or loyalty card application, or understood what they were consenting to.

As a result of the above, I am satisfied that the personal health information of these complainants was not used and/or disclosed by agents of these other hospitals for the purposes of selling or marketing RESPs and each of these files has been closed.

ISSUES

In this Order, I will consider the following issues:

- a) Is the information at issue "personal health information" as defined in section 4 of the *Act*?
- b) Is the person who operates the Hospital a "health information custodian" as defined in section 3(1) of the *Act*?
- c) Were Employee 1 and Employee 2 "agents" of the Hospital as defined in section 2 of the *Act*?
- d) Was personal health information "used" and/or "disclosed" in accordance with the *Act*?
- e) Did the Hospital take steps that are reasonable in the circumstances to ensure that person-

al health information in its custody or control is protected against theft, loss and unauthorized use or disclosure in accordance with section 12(1) of the *Act*?

- f) Did the Hospital have in place information practices that comply with the *Act* and did it comply with these practices in accordance with section 10(1) and 10(2) of the *Act*?

RESULTS OF THE INVESTIGATION

Issue A: Is the information at issue “personal health information” as defined in section 4 of the *Act*?

Section 4(1) of the *Act* states, in part:

In this *Act*,

“personal health information”, subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information,

(a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family,

(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,

...

(f) is the individual’s health number, or

(g) identifies an individual’s substitute decision-maker.

Section 4(2) of the *Act* states:

In this section,

“identifying information” means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

In its representations, the Hospital stated that it does not know the exact nature and type of information that was used and/or disclosed by Employee 1 and Employee 2. Based on the information available to the Hospital, the Hospital “surmises that the information used and/or disclosed by the Employees was: patient names of the mother and baby, baby’s gender, baby’s date of birth, and the mother’s telephone number.”

The Hospital acknowledges that this information is “personal health information” as that term is defined in the *Act*. In its representations, the Hospital states that section 32(2) of the *Act* suggests that an individual’s name and contact information constitute “personal health information” even if they do not on their own relate to the physical or mental health of the individual, the health history of the family or the provision of health care to the individual.

I find that the information at issue is “personal health information” as defined in section 4 of the *Act*. It identifies the name of the mother and the baby and identifies that the mother and baby were patients of the Hospital. Section 4(1) of the *Act* clearly states that personal health information includes the identification of a person, in this case the Hospital, as a provider of health care to the individual, in this case the mother and the baby.

Issue B: Is the person who operates the Hospital a “health information custodian” as defined in section 3(1) of the Act?

Section 3(1) of the *Act* states, in part:

“health information custodian”, subject to subsections (3) to (11), means a person or organization described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person’s or organization’s powers or duties or the work described in the paragraph, if any:

...

4. A person who operates one of the following facilities, programs or services:

i. A hospital within the meaning of the *Public Hospitals Act*...

Section 2 of the *Act* defines a “person” to include a partnership, association or other entity. Section 87 of the *Legislation Act* further provides that a “person” includes a corporation.

Consistent with the IPC’s findings in previous Orders, I find that the Hospital is a “person” who operates a hospital within the meaning of the *Public Hospitals Act* and that it is a health information custodian with custody or control of the personal health information at issue as defined in section 3(1)4i of the *Act*. The Hospital does not dispute this finding.

Issue C: Were Employee 1 and Employee 2 “agents” of the Hospital as defined in section 2 of the Act?

The issue to be decided here is whether Employee 1 and Employee 2 were “agents” when they used and/or disclosed personal health information in the custody or control of the Hospital for the purposes of selling or marketing RESPs. The issue is relevant to determining whether the

personal health information was “used” and/or “disclosed” within the meaning of the *Act*.¹

Section 2 of the *Act* defines an “agent” as:

“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.

The Hospital submits that Employee 1 and Employee 2 were not “agents” for these purposes. The Hospital argues that it did not authorize Employee 1 or Employee 2 to use and/or disclose personal health information for the purposes of selling or marketing RESPs and, in doing so, the Employees acted beyond the authority delegated by the Hospital. It argues that these uses and/or disclosures of personal health information by the Employees were not in the course of their duties and were not carried out for, or on behalf of and for the purposes of, the Hospital, but rather, were “clearly motivated by self-interest.” Therefore, the Hospital argues that the Employees were not “agents” within the meaning of the *Act* in using and/or disclosing personal health information for these purposes.

Having carefully considered these representations, I disagree. In the usual course of their duties, Employee 1 and Employee 2 acted for or on behalf of, for the purposes of and with the authorization of the Hospital in respect of personal health information, and not for their own purposes. They were authorized to collect, use, disclose, retain or dispose of personal health information to assist the Hospital in carrying out its duties. Therefore, they were “agents” under the *Act* even though they may have acted beyond the authority delegated by the Hospital in the particular instances when they used and/or disclosed personal health information to market or sell RESPs.

This interpretation is consistent with previous Orders of the IPC. As held in Orders HO-002 and HO-010:

A cursory reading of the definition of “agent” in the circumstances of this complaint might suggest that, because in this instance the nurse did not have the hospital’s authorization to use or disclose the health information in question, and was in fact doing so for her own purposes, she was not an “agent.” That is not my view. For the reasons that follow, I have concluded that this interpretation is not sustainable, and that the nurse was in fact an agent.

¹ The provision 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. See section 6(1) of the *Act*.

A careful reading of the definition, particularly when viewed in the context of the *Act* as a whole, makes it clear that the Legislature intended that the phrase, “acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian” should be read as a reference to the person’s *usual* duties and activities, as opposed to an action taken in the particular circumstances of a complaint... It is also important that the definition of “agent” expressly contemplates the inclusion of employees in this category.²

My finding is also supported by the modern rule of statutory interpretation which states: “the words of an Act are to be read in their entire context, in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.”³

Grammatical and Ordinary Meaning of “Agent”

In *R v Conception*, the Supreme Court of Canada emphasized that the starting point of statutory interpretation “is the text of the provisions in their grammatical and ordinary sense,” especially where the key term is expressly defined by statute.⁴ Section 2 of the *Act* defines an “agent” as “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.”

The Hospital argues that the Employees were not acting “with the authorization of” and “for or on behalf of” and “for the purposes of” the Hospital, but rather for their “own purposes,” and therefore were not “agents” within the meaning of the *Act* in using and/or disclosing personal health information for the purposes of selling or marketing RESPs.

I do not agree with this position. Employee 1 and Employee 2 meet the definition of “agent” in the ordinary sense of the word used in the *Act*. They are “persons” who acted “with the authorization of,” “for or on behalf of,” and “for the purposes of” the Hospital in respect of personal health information in the usual course of their duties. But for the fact that they were agents, the Employees would not have had access to the personal health information at issue.

² (July 2006), HO-002, online: IPC <http://www.ipc.on.ca/images/Findings/up-HO_002.pdf> at 5 [HO-002]; (December 31, 2010), HO-010, online: IPC <<http://www.ipc.on.ca/images/Findings/ho-010.pdf>> at 7 [HO-010].

³ Ruth Sullivan, *Sullivan on the Construction of Statutes*, 5th ed (Markham: LexisNexis Canada Inc., 2008) at 1; *Re Rizzo & Rizzo Shoes Ltd.*, [1998] 1 SCR 27 at para 41; and *R. v. Conception*, 2014 SCC 60 at para 14 [*Conception*].

⁴ *R. v. Conception*, *supra* note 3.

This interpretation is consistent with the grammatical and ordinary meaning of the term “agent.” “Agent” is defined by Merriam-Webster as “a person who does business for another person,” “a person who acts on behalf of another,” or “a person or thing that causes something to happen.”⁵ Similarly, Oxford defines “agent” as “a person who acts on behalf of another” or “a person or thing that takes an active role or produces a specified effect.”⁶ None of the dictionary definitions consulted indicate that a person must act within the authorization of, for or on behalf of and for the purposes of the other person *at all times* in order to be an agent.

The words “with the authorization of the custodian,” “acts for or on behalf of the custodian,” and “for the purposes of the custodian, and not the agent’s own purposes” in section 2 of the *Act* ensure that third parties who do not have an employment, contractual or other agency relationship with the custodian fall outside the scope of the definition of “agent.” These words make it clear that third parties who may be permitted to access personal health information in health care settings for their own purposes, such as independent researchers, assessors or inspectors of regulatory colleges and government inspectors, are not “agents” within the meaning of the *Act* and therefore the custodian is not responsible for their actions in respect of the personal health information in its custody or control.

Objects and Scheme of the Act

The *Legislation Act* states that a statute shall be interpreted as being remedial and shall be given “such fair, large and liberal interpretation as best ensures the attainment of its objects.”⁷

The Hospital’s argument that the term “agent” should be narrowly interpreted to exclude a person who is authorized to collect, use, disclose, retain or dispose of personal health information for or on behalf of and for the purposes of a health information custodian in the usual course of his or her duties, but who, in a particular instance or instances, collects, uses, discloses, retains or disposes of that information for an unauthorized purpose, is inconsistent with the objects of the *Act* and with the scheme of the *Act*.

Objects of the Act

The objects of the *Act* are set out in section 1, which provides in part:

⁵ *Merriam-Webster Online Dictionary*, *sub verbo* “agent.”

⁶ *Oxford Online Dictionary*, *sub verbo* “agent”; likewise, *Cambridge Dictionaries Online*’s definition of “agent” includes “a person who acts for or represents another”, *sub verbo* “agent.”

⁷ *Legislation Act, 2006*, SO 2006, c 21 Sched F at s 64(1).

1. The purposes of this *Act* are,

(a) 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 with respect to that information, while facilitating the effective provision of health care;

[...]

(e) to provide effective remedies for contraventions of this *Act*.

At its core, the objects or purposes of the *Act* are to protect the privacy of individuals in respect of their personal health information, to protect the confidentiality of that information and to provide effective remedies for contraventions of the *Act*. Privacy and confidentiality are best protected by holding health information custodians accountable for the conduct of persons who act for or on their behalf and for their purposes in the usual course of their duties.

As the law of vicarious liability demonstrates, “[e]mployers are often in a position to reduce accidents and intentional wrongs by efficient organization and supervision.”⁸ Vicarious liability is designed to ensure that the employer remains responsible for the reasonably foreseeable risks attributable to or arising from the employer’s activities so that the employer takes reasonable steps to reduce the risk. This has been acknowledged on numerous occasions by the Supreme Court of Canada. In *London Drugs v Kuehne & Nagel International Ltd.*, the Court noted “[v]icarious liability has the broader function of transferring to the enterprise itself the risks created by the activity performed by its agents.”⁹ Further, in *John Doe v Bennett*, the Court stated “the hope is that holding the employer or principal liable will encourage such persons to take steps to reduce the risk of harm in the future.”¹⁰

But for the fact that they were employees, Employee 1 and Employee 2 would not have had access to the personal health information at issue. Therefore, the Hospital provided the opportunity and created the risk of unauthorized use and disclosure. The Hospital is also in the best position to take reasonable steps to reduce the risk of further contraventions of the *Act* not only by Employee 1 and Employee 2, but by all persons. The Hospital, and not the Employees, can develop, amend and implement policies, procedures, practices and safeguards that apply to all persons, including those acting for or on its behalf and for its purposes in the usual course of their duties.

⁸ *Bazley v Curry*, [1999] 2 SCR 534 at para 32.

⁹ [1992] SCR 299 at 339.

¹⁰ 2004 SCC 17 at para 20.

If the Hospital's submissions were accepted, a health information custodian would arguably have less responsibility for those acting for or on its behalf and for its purposes in the usual course of their duties under the *Act* than under the law of vicarious liability. This clearly does not protect the privacy of individuals with respect to their personal health information and the confidentiality of that information. If the Legislature intended to limit the responsibility of health information custodians for the actions of those acting for or on their behalf in the usual course of their duties, it would have included clear and unambiguous language in the *Act*. Absent such clear and unambiguous language, there is no basis for interpreting the term "agent" in such a way that is fundamentally inconsistent with the purposes of the *Act*.

The Hospital argues that "it is not necessary for a person to be an 'agent' to be covered by the restrictions and potential sanctions in the *Act*." In particular, it argues that the Commissioner may make an order under section 61(1) of the *Act* against "any person" and that "any person" may be charged with an offence under section 72 of the *Act*, suggesting that such orders and prosecutions would, in these circumstances, achieve the objects or purposes of the *Act*.

While an order of the Commissioner directed at "any person" or a prosecution commenced by the Attorney General against "any person" may have a deterrent effect on others, such measures would not adequately address the systemic issues that an order directed at a health information custodian would achieve. As previously noted, an order directed at a custodian to implement policies, procedures, practices and safeguards would reduce the risk of further contraventions of the *Act* not only by the "person" whose acts or omissions are at issue, but all "persons" acting for, on behalf of and for the purposes of the custodian in the usual course of their duties.

There are further problems with the Hospital's proposed interpretation. If the Hospital's submissions were accepted, it would result in inconsistent treatment or accountability of health information custodians under the *Act*, depending on whether or not they act through other persons. For example, custodians that are corporations (such as community care access corporations and corporations that operate hospitals, long-term care homes and pharmacies) and other custodians that act through other persons would have less responsibility for contraventions of the *Act* than a custodian who may do so to a lesser degree, such as a sole health care practitioner. Such an interpretation is inconsistent with the objects and purposes of the *Act*.

Moreover, if the Hospital's submissions were accepted, it would result in persons constantly transitioning between acting as agents and non-agents, potentially from one moment to the next, throughout the course of a day. The effort that would be required to determine exactly when each person was acting as an agent would create unnecessary confusion and ultimately frustrate the ability of the Commissioner and the courts to achieve the objects and purposes of the *Act*.¹¹ The objects and purposes of the *Act* are not to apportion liability between the

¹¹ This type of impractical time-based interpretation was expressly criticized in reference to the *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F-31, in *Ontario (Solicitor General) v Mitchinson*, (2001) 55 OR (3d) 355 (CA), [2001] OJ No 3223 at paras 38-40.

health information custodian and persons acting for or on its behalf. Its main object or purpose is to protect privacy and confidentiality of individuals in a health care setting.

Scheme of the Act

My finding as to the proper interpretation of the term “agent” in section 2 of the *Act* is also consistent with other provisions in the *Act*.

Section 17(1) provides, in part, as follows:

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 ...

This section unequivocally states that a health information custodian is responsible for personal health information in its custody or control. A health information custodian may permit others to collect, use, disclose, retain or dispose of personal health information for or on its behalf, but the *Act* clearly states that the custodian remains responsible. Nothing in the *Act* permits a custodian to delegate or assign that responsibility.

In these circumstances, there is no dispute that the personal health information at issue was and continues to be in the custody and control of the Hospital. Therefore, pursuant to section 17(1), as the health information custodian, the Hospital “is responsible” for that information.

In fact, the majority of the obligations under the *Act* are imposed on health information custodians, not on other persons, including agents. This clearly points to the fact that accountability for personal health information remains with the custodian.

The Hospital’s suggestion that a person is not an “agent” when they act beyond the authority delegated by the Hospital is also inconsistent with sections 17(1)(b) and (2), which state:

- (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,

...

(b) the collection, use, disclosure, retention or disposition of the information, as the case may be, is in the course of the agent’s duties and not contrary to the limits imposed by the custodian, this *Act* or another law; and
- (2) Except as permitted or required by law and subject to the exceptions and additional requirements, if any, that are prescribed, an agent of a health information custodian shall not collect, use, disclose, retain or dispose of personal health information on the custo-

dian's behalf unless the custodian permits the agent to do so in accordance with subsection (1).

Section 17(2) of the *Act* expressly permits agents to collect, use, disclose, retain or dispose of personal health information without the permission or authorization of the health information custodian in certain circumstances, including those prescribed in section 7 of Regulation 329/04 under the *Act*.¹² As a result, the *Act* clearly contemplates that a person does not cease to be an agent simply because the custodian did not permit or authorize the agent to collect, use, disclose, retain or dispose of personal health information for a specific purpose. In addition, sections 17(1)(b) and (2) clearly contemplate the possibility of unauthorized collection, use, disclosure, retention or disposal by agents, which would be impossible if the Hospital's submissions were accepted. As stated in both Orders HO-002 and HO-010:

Section 17 of the *Act* clearly contemplates the possibility of improper collection, use or disclosure by agents, which would be impossible if their status as agents ended when they ceased acting for the custodian's purposes and began acting for their own... these provisions would be rendered meaningless if a person who would usually be an agent is converted to a non-agent in the event that they act improperly. The Legislature could not possibly have intended this result.¹³

The Hospital refers to section 12(2) of the *Act* in support of its position that Employee 1 and Employee 2 were not "agents" when they used and/or disclosed personal health information for the purposes of selling or marketing RESPs. Section 12(2) states:

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.

The Hospital states that an agent is by definition not "an unauthorized person" and therefore suggests that because the Hospital was required to notify affected individuals under section 12(2), the Employees could not possibly have been agents.

Again, I do not agree. If the position of the Hospital were accepted, a health information custodian would also not be required to notify affected individuals under section 12(2) if the custodian authorized a person to use and/or disclose personal health information in contravention of the *Act* on the basis that the personal health information would not have been "accessed by an

¹² *Personal Health Information Protection Act, 2004*, Ontario Regulation 329/04 at s 7.

¹³ Orders HO-002 and HO-010, *supra* note 2.

unauthorized person.” Such a result would not conform with the scheme of the *Act*.

Section 12(2) cannot be read in isolation. It must be read in the context of the section in which it is found as well as the other provisions of the *Act*. The immediately preceding section 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.

The notice requirement in section 12(2) of the *Act* stems from the obligation in section 12(1) which requires a health information custodian to take steps that are reasonable in the circumstances to protect personal health information against “unauthorized use or disclosure.” Section 12(2) should be interpreted to encompass unauthorized use or disclosure of personal health information.

The Legislative Intent

The Hospital has not referenced any legislative history to support its narrow interpretation of the term agent.” In fact, the legislative history supports a broad interpretation.

Statements made by individuals who were instrumental in advising the Ministry of Health and Long-Term Care (the Ministry) on the development of the *Act*, make it clear that the term “agent” is to be interpreted broadly. For example, when explaining the term “agent” to the Standing Committee considering the bill that led to the *Act*, legal counsel for the Ministry stated:

There’s always someone who is responsible. The hospital is responsible for all the health-care practitioners who work within it. As well, the doctor is responsible for his or her own staff in the office... *The definition of “agent” is an expansive definition.* It includes students, it would include volunteers; it is all of those who work within a custodian.¹⁴

Before the same committee, the Acting Director of the Health Information, Privacy and Sciences Branch of the Ministry confirmed the breadth of the definition of “agent” in the *Act*:

You’ll see in section 17 the point that we made earlier, that custodians are responsible for the actions of their agents. Whether it’s a volunteer working in a hospital or an information manager that you’ve hired to transcribe your records,

¹⁴ Ontario, *Standing Committee on General Government (Hansard)*, 38th Parl, 1st Sess, (January 26, 2004) at 1050 (Halyna Perun) [emphasis added].

ultimately, the custodian is responsible.¹⁵

In fact, the definition of “agent” was further broadened by the Standing Committee to include the phrase “whether or not the agent has the authority to bind the custodian,”¹⁶ which is how the term is currently defined in section 2 of the *Act*. The Standing Committee’s expansion of the definition is further evidence that the term “agent” is meant to be interpreted broadly.

Upon consideration of the grammatical and ordinary meaning of “agent,” the objects and scheme of the *Act* and the legislative intent, I find that Employee 1 and Employee 2 were “agents” of the Hospital in the particular instances when they used and/or disclosed personal health information for the purposes of selling or marketing RESPs.

Issue D: Was personal health information “used” and/or “disclosed” in accordance with the Act?

Section 2 of the *Act* defines “use” and “disclose” as follows:

“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;

“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;

Section 6(1) of the *Act* is also relevant. It states, in part, that “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...”

Personal health information is permitted to be used or disclosed if the use or disclosure complies with section 29 of the *Act*, which states:

A health information custodian shall not collect, use or disclose personal health

¹⁵ Ontario, *Standing Committee on General Government (Hansard)*, 38th Parl, 1st Sess, (January 26, 2004) at 1110 (Carol Appathurai).

¹⁶ Ontario, *Standing Committee on General Government (Hansard)*, 38th Parl, 1st Sess, (April 28, 2004) at 1600 (Kathleen Wynne).

information about an individual unless,

- (a) it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or
- (b) the collection, use or disclosure, as the case may be, is permitted or required by this Act.

As previously discussed, in July 2013, Employee 1 was transferred to another department at the Hospital's Centenary site and his access rights to personal health information in the Meditech system were terminated. According to the information provided by the Hospital, Employee 1 asked his manager to reinstate his previous access rights and stated that he had been accessing the Meditech system to obtain the contact information of new mothers so that he could contact them for the purposes of selling them RESPs. Following an investigation by the Hospital, the Hospital concluded that there had been a violation of the Hospital's privacy policy and of the *Act* and reported the breach to the IPC. The Hospital has indicated to the IPC that it has no information to suggest that Employee 1 disclosed personal health information.

Employee 2 admitted that she accessed personal health information for the purpose of selling it to an RESP sales agent and sold that information to the RESP agent for that purpose, and that she had been doing so since 2010. Employee 2 sold the personal health information knowing that the RESP agent was using this information to sell or market RESPs to patients.

Employee 2 used the Meditech scheduling module to search the patient index and retrieve the contact information of the patients. The printouts of Meditech screen shots found in April 2014 show that Employee 2 was able to return a list of newborns by searching for a patient with the name "AA" and a recent date of birth. Because the name "AA" did not match any patients in the patient index, the system relaxed the search criteria and searched for any patients with the specified date of birth only. In this way, an open-ended search for newborns was performed. By selecting the name of a newborn from the results of the patient index search, Employee 2 was able to access information about the newborn's mother.

Use of Personal Health Information

Based on the information provided by the Hospital and the information gathered in this review, and given that I have found that the Employees were agents of the Hospital, applying section 6(1) of the *Act*, I find that their handling and dealing with the personal health information described above was a "use" within the meaning of section 2 of the *Act*. I also find that this use of personal health information was for the purposes of selling or marketing RESPs or for the purpose of selling the personal health information to an RESP sales agent who in turn was selling or marketing RESPs to patients.

There is no information or evidence before me to suggest that patients consented to this use of

their personal health information. In addition, no section in the *Act* permits or requires such a use of personal health information without the consent of patients. Section 37 of the *Act* sets out the purposes for which personal health information is permitted to be used without consent. I find that none of these purposes applies in the circumstances before me.

The Hospital acknowledges that personal health information was used without patient consent and that this use was not permitted by section 37 of the *Act*. In its representations, the Hospital states “the Employees used [personal health information]. They did not have patient consent to do so and were not using the [personal health information] for any purpose permitted under section 37 of [the *Act*] or permitted by the Hospital.”

Not only does the *Act* not permit or require such a use of personal health information without consent, the *Act* prohibits such a use. Section 33 of the *Act* states:

A health information custodian shall not collect, use or disclose personal health information about an individual for the purpose of marketing anything or for the purpose of market research unless the individual expressly consents and the custodian collects, uses or discloses the information, as the case may be, subject to the prescribed requirements and restrictions, if any.

Therefore, I find that the use of personal health information for the purposes of selling RESPs or for the purpose of selling the personal health information to an RESP sales agent who in turn was selling or marketing RESPs to patients was not permitted and, in fact, was expressly prohibited without express consent, and therefore contravened section 29 of the *Act*.

Disclosure of Personal Health Information

Based on the information provided by the Hospital, there is no evidence to suggest Employee 1 disclosed personal health information. However, as acknowledged by the Hospital, Employee 2 admitted that she provided personal health information to an RESP sales agent for the purpose of selling or marketing RESPs. I find that in making this information available or releasing it to an RESP sales agent, personal health information was “disclosed” within the meaning of section 2 of the *Act*. I also find that this disclosure of personal health information was for the purposes of selling or marketing RESPs.

There is no information or evidence before me to suggest that patients consented to this disclosure of their personal health information. In fact, the Hospital states that “Employee 2 did not obtain patient consent” for the disclosure.

In addition, no section in the *Act* permits or requires such a disclosure of personal health information without the consent of patients. Sections 38 - 50 of the *Act* set out the purposes for which personal health information is permitted to be disclosed without consent. I find that none of these purposes applies in the circumstances before me. Not only does the *Act* not permit or require such a disclosure of personal health information without consent, but as noted above,

section 33 of the *Act* expressly prohibits such a disclosure.

Therefore, I find that the disclosure of personal health information for the purpose of selling or marketing RESPs to patients was not permitted and, in fact, was expressly prohibited without express consent, and therefore contravened section 29 of the *Act*.

While I previously found that both Employees were agents of the Hospital within the meaning of section 2 of the *Act*, if they were not agents for these purposes, as argued by the Hospital, the provision of personal health information to them would have been disclosures to them by the Hospital. Consistent with my previous findings, such disclosures were not made with the consent of patients and were not permitted or required by the *Act* and, in fact, were expressly prohibited. Therefore, I find that even if the Employees were not agents of the Hospital for these purposes, these disclosures would have contravened section 29 of the *Act*. Therefore, regardless of whether the Employees were agents of the Hospital for these purposes, and regardless of whether the provision of personal health information by the Hospital to them were “uses” or “disclosures,” the Hospital is responsible for such uses or disclosures.

Issue E: Did the Hospital take steps that are reasonable in the circumstances to ensure that personal health information in its custody or control is protected against theft, loss and unauthorized use or disclosure in accordance with section 12(1) of the Act?

Section 12(1) of the *Act* sets out the obligation of health information custodians to implement steps that are reasonable in the circumstances to protect personal health information against unauthorized use or disclosure. It states:

A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

In Order HO-010, the IPC stated that measures or safeguards must be reviewed from time to time to ensure that they continue to be “reasonable in the circumstances” in order to protect personal health information from theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal. As new technologies are developed, adopted or implemented and as new threats and vulnerabilities emerge, “steps that are reasonable in the circumstances,” the standard in section 12(1) of the *Act*, will also evolve.

This means that, among other things, health information custodians must identify the risks to privacy and confidentiality of personal health information and implement measures or safeguards that are reasonable in the circumstances to eliminate or reduce these risks and to mitigate the harms that may arise from these risks. The risks to privacy and to the confidentiality of personal health information posed by agents who use or disclose personal health information for purposes that contravene the *Act* are well known. The IPC has issued two previous Orders¹⁷ and other privacy commissioners have issued a number of orders or reports stemming from this issue.¹⁸ Articles in major newspapers evidence increased public concern over this issue and its impact on patients.¹⁹ There have been a number of prosecutions of agents for uses and disclosures in contravention of privacy legislation in other provinces. In Ontario, the Attorney General has commenced a prosecution against a nurse who worked at a hospital in northern Ontario for allegedly accessing the personal health information of more than 5,000 patients in contravention of the *Act*. This prosecution is ongoing.²⁰

Accordingly, in my view, the Hospital should have known about the risks to privacy and to the confidentiality of personal health information posed by its own agents before the first breach was discovered in 2013 and should have taken steps that were reasonable in the circumstances, as outlined below, before that time. Its failure to do so contravened section 12(1) of the *Act*. Even if the Hospital was not aware of this risk prior to the time the first breach was discovered, it should have become aware of the risk at that time. In addition, after the first breach, the Hospital clearly knew or ought to have known that it did not have in place sufficient measures or safeguards to detect or confirm uses and disclosures of personal health information in contravention of the *Act* by agents using the Meditech scheduling module. Based on this, I find that even if the Hospital did not contravene section 12(1) of the *Act* prior to discovering the first breach in 2013, the Hospital contravened section 12(1) of the *Act* when it failed to take steps that were reasonable in the circumstances, as outlined below, after that time.

The Hospital states that it has complied with section 12(1) because the Hospital “has taken steps that are reasonable in the circumstances, as measured against Ontario health sector

¹⁷ Orders HO-002 and HO-010, *supra* note 2.

¹⁸ Investigation Report H-2013-001 Office of the Information and Privacy Commissioner-Saskatchewan, 2013 CanLII 5640 (SK IPC); Investigation Report H2011-IR-004 Information and Privacy Commissioner of Alberta, <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2912>; Manitoba Ombudsman Report 2011-0513 and 2011-0514, <https://www.ombudsman.mb.ca/uploads/document/files/cases2011-0513-0514-en.pdf>.

¹⁹ See Olivia Carville, “Hospital Privacy Violations Rife in Ontario,” *The Toronto Star*, October 29, 2014, (URL)

²⁰ See Maria Calabrese, “Hospital Defends Private Records,” *North Bay Nugget*, June 12, 2013, <http://www.nugget.ca/2013/06/11/hospital-defends-private-records>.

practices and more specifically the practices of other similarly situated (size, region, resources) public hospitals and the information technology assets at the Hospital's disposal." It states that "the Hospital's safeguards to protect [personal health information] have been tested at different times against the requirements established for regional information technology initiatives," and refers to the Hospital Diagnostic Imaging Repository Services as an example. It also states that it uses a standard configuration of the Meditech system and the same safeguards used by other Meditech clients and added that any new audit functionality that it implemented following the first reported breach is a "custom feature."

The health information custodian has the onus of establishing compliance with section 12(1) of the *Act*. While the Hospital claims that it has complied with section 12(1), it has not provided me with any information or evidence to support its claims about the practices in place in the Ontario health sector. Nor has it explained how its safeguards "have been tested" against "the requirements established for regional information technology initiatives," including the Hospital Diagnostic Imaging Repository Services. Nor has it provided me with any information or evidence about the safeguards used by other Meditech clients, other than its Hosting Provider. Even if it had provided information to support these claims, these factors would not be determinative of the question of whether the Hospital has complied with its obligations under section 12(1).

Below I provide further details of the deficiencies in the Hospital's compliance with section 12(1). These deficiencies are addressed in the following two general headings, Technical Measures or Safeguards and Administrative Measures or Safeguards.

Technical Measures or Safeguards

Audit Functionality

As in other industries, audits play an important role in the health sector. 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 infor-

mation custodian will not be able to conduct a complete audit in relation to the personal health information stored in its electronic information system.

As noted above, the two Employees had access to the scheduling module of the Hospital's Meditech system which contains the personal health information of patients, including new mothers. The scheduling module provides access to demographic information about patients such as their name, address and phone numbers, as well as information about their date of birth, health number and the dates of visits to the Hospital.

In the Meditech system, analyzable data about user activities within the scheduling module is generated in the form of user activity logs. As the name suggests, these logs, if available, can be used to create an audit report of user activities.

User activity logs are not the only means of conducting audits in the Hospital's Meditech system. For example, the Hospital states that it is able to audit the activities of users by generating "system utilization reports" which capture user access to personal health information in the Patient Care Inquiry (PCI) module. Although they are important elements of the Hospital's overall auditing system, system utilization reports are specific to the PCI module and do not capture information about access to personal health information within the scheduling module. As such, these reports do not address the personal health information at issue in this review. The only means of conducting audits on user activities within the scheduling module are user activity logs, which, according to the Hospital, are different from system utilization reports.

Having carefully reviewed the information provided by the Hospital in response to the Notice of Review and the Supplementary Notice of Review, I find that the Hospital did not take steps that were reasonable in the circumstances with respect to the audit functionality of the scheduling module of the Meditech system and therefore failed to comply with section 12(1). In particular, I take issue with three aspects of the Hospital's auditing functionality: the user activity log history, the service level agreement and the user activity log information. With respect to each of these aspects, the reasons for my finding of non-compliance are as follows:

User activity log history. At the time of the first reported breach, the Hospital's Meditech system did not archive user activity logs for a period longer than 14 days. This meant that the Hospital was unable to conduct any audits of user activities within the scheduling module that occurred more than two weeks prior.

Service level agreement. The service level agreement between the Hospital and the Hosting Provider did not include a requirement for the Hosting Provider to ensure that user activity logs generated by the Hospital's users were archived and available to the Hospital for auditing purposes.

User activity log information. In its report to this office following the first reported breach, the Hospital committed to addressing the lack of user activity logs by ensuring that user activity logs were permanently archived and available to the Hospital for audit purposes. However, despite this improvement, it became apparent during this review that the

Hospital was still unable to audit Employee 2's activities within the scheduling module because the user activity logs generated by its Meditech system lacked key information. Specifically, the user activity logs did not capture the selection of a patient's name on the patient index within the scheduling module. The Hospital came to this realization only after the second reported breach whereas it should have discovered this shortcoming in its auditing system immediately after the first reported breach and taken the appropriate actions to address it at that time.

User Activity Log History

As I indicated above, the Hospital shares a version of Meditech software with another hospital, which is referred to throughout this Order as the Hosting Provider. The Hosting Provider owns the license for the software and is responsible for implementing and operating a Meditech system on behalf of the Hospital. The Hospital is entitled to use the Meditech system pursuant to a service level agreement which sets out the roles and responsibilities of the parties in relation to the Meditech system and the information stored in the system.

At the time of the first reported breach, the Hospital's Meditech system was configured to retain user activity logs for a maximum period of 14 days. This meant that any audit log information about users' activities within the scheduling module was automatically overwritten if the activities were older than 14 days.

In addition, these logs were not archived by the Hosting Provider so as to enable their long-term storage and retrieval for audit or any other purposes. Thus once overwritten, any audit log information about user activities within the scheduling module was permanently deleted. Since the Meditech system is shared between the Hospital and the Hosting Provider, this included the user activity logs for the Hospital.

Upon discovery of the first reported breach, the Hospital became aware of these limitations in the auditing functionality of its Meditech system and that it was unable to perform an audit of Employee 1's activities.

One consequence of this lack of user activity logs and the inability to conduct an audit of user activities within the scheduling module was that the Hospital was unable to identify the patients whose personal health information was accessed. This was confirmed in a letter from the Hospital to the IPC dated October 8, 2013, stating that "[d]ue to the fact that we were not able to view patient record level audit logs we were not able to quantify the number of patients whose information was viewed inappropriately [...]."

During our investigation into the first reported breach, the Hospital committed to addressing the archiving limitations in the auditing functionality of its Meditech system. In the same October 8, 2013 letter, the Hospital states:

In order to overcome the audit log limitation that we discovered in our Meditech

system, we are working with our hosting party, [], and the vendor, Meditech, on two enhancements of the access logs: (a) extend the length of the live Meditech log to ninety days and enable the archiving of the logs past ninety days, (b) create an export of the access logs from the Meditech proprietary format to a relational database that will allow us to maintain unlimited access history and report inappropriate access.

In its representations, the Hospital was given an opportunity to explain its position in regards to this lack of auditing capabilities at the time of the first reported breach. When asked specifically why, at the time of the first reported breach, user activity logs were not archived, the Hospital replied that “[it] did not have the option of archiving logs because it does not own the Meditech Archiving Module (MAM).”

This answer is unacceptable. As a custodian of personal health information, the Hospital is responsible for personal health information in its custody or control. The fact that it does not “own the Meditech Archiving Module” does not absolve it of its responsibilities under the *Act*. In the words of a former Commissioner, “you can outsource services, but you cannot outsource accountability.”²¹ Regardless of who is actually implementing and operating the Meditech system, the Hospital is responsible for ensuring that measures or safeguards that are reasonable in the circumstances are in place to protect personal health information in its custody or control against theft, loss and unauthorized use or disclosure and to protect records of personal health information in its custody or control against unauthorized copying, modification or disposal. If the Hosting Provider was responsible for maintaining and archiving user activity logs, then the service level agreement should have reflected that. If the Hosting Provider was not responsible for maintaining those logs, then the Hospital should have taken steps to ensure that it maintained the logs through other means.

Service Level Agreement

The Hospital’s position in regard to its lack of auditing capabilities at the time of the first reported breach raised the question of the adequacy of the service level agreement and whether it complied with section 12(1) of the *Act*. The service level agreement stipulates that the Hospital’s “Meditech databases” will be “independent” of the Hosting Provider’s; that the Hospital “owns” the “data contained within [its] databases;” and that the Hosting Provider is responsible for maintaining the security, confidentiality and integrity of the Hospital’s “data” by providing controlled access to it and performing daily backups of it.

While the service level agreement contains many provisions that stipulate much of the required functionality of the shared Meditech system, it does not address the responsibility for ensuring

²¹ *Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report*, June 27, 2012, http://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf, p. 6.

that the user activity logs generated by the Hospital's use of its Meditech system are archived and available to the Hospital for auditing purposes.

In particular, the service level agreement does not contain a provision that explicitly sets down the requirements for logging the activity of agents or users and the archiving of user activity logs generated by the Meditech system. Indeed, the service level agreement makes no mention at all of "user activity logs" or even "audit logs."

Second, where the service level agreement discusses the Hosting Provider's requirement to "perform [] daily backups of the software and data," it is not clear whether these daily backups include backups of user activity logs.

In Order HO-010, issued in December 2010, the IPC dealt with a complaint related to the use of personal health information by a technologist at The Ottawa Hospital without consent and in contravention of the *Act*. During the IPC's review, it was determined that one of the hospital's electronic information systems included audit functionality, but that it had not been turned on. With respect to the obligations imposed pursuant to section 12(1), the IPC found:

The fact that audit functions are either non-existent or have not been turned on in relation to any of the electronic information systems of the hospital that contain personal health information falls short of meeting the requirements of section 12(1) of the *Act*.

I agree. I find that the Hospital's failure to ensure that user activity logs were available to conduct audits was a contravention of section 12(1) of the *Act*.

Although the Hospital states that it has taken steps to address the limitations in its auditing system such that it no longer relies upon the Hosting Provider for the archiving of user activity logs, in the Order provisions that follow, I will require the Hospital to work with the Hosting Provider to review and amend the service level agreement between the Hospital and the Hosting Provider to clarify the responsibility for the creation, maintenance and archiving of user activity logs generated by the Hospital's use of its Meditech system, and to ensure that the user activity logs are available to the Hospital for audit purposes.

User Activity Log Information

As noted above, in the case of both breaches, the two Employees had access to the scheduling module of the Hospital's Meditech System. Employee 2 used and/or disclosed the personal health information about new mothers by selecting their name or the name of their newborn from the results of a patient index search within the scheduling module.

In the Meditech system, when a patient name is selected from the results of a patient index search, additional information about that patient is displayed at the bottom of the screen. This information includes the patient's address, phone number, health number, and a list of dates of Hospital visits. This information is provided for verification purposes, i.e., so that the user can

confirm that the selected patient is in fact the patient the user is searching for. Thus, alongside the information about the patient displayed at the bottom of the screen, a dialog box appears to the user. The dialog box prompts the user with the question “Is this the one?” and gives the user the option of answering “Yes” or “No.”

If the user selects “Yes,” then the selected “patient’s record” is shown. However, if the user selects “No,” the user is taken back to the results of the patient index search. A key configuration of the Hospital’s Meditech system is that it is only when the user goes on to view the selected “patient’s record” (by selecting “Yes” in the dialog box) that an event regarding the user’s access to that patient’s personal health information is recorded in the user activity log. If the user clicks “No,” then an event regarding the access to that patient’s personal health information is not recorded in the user activity log, despite the fact that the user was able to view the patient’s personal health information displayed at the bottom of the screen. In its representations, the Hospital explained this aspect of its auditing system as follows:

If the user selects to proceed once the user has determined from the demographic information that the patient is the correct patient, by clicking “Yes” in the dialogue box entitled “is this the right one,” the user triggers an audit trail. If the user clicks “No,” there is currently no audit trail.

In the case of the first breach, this limitation in the Hospital’s auditing capabilities did not affect its ability to perform an audit on Employee 1, since, as noted above, the short retention period and lack of archiving of audit logs ruled out the possibility of conducting an audit on Employee 1’s activities within the scheduling module.

However, in the case of the second breach, this limitation played an important role. At the time of the second breach, the Hospital had roughly six months of audit logs available to it. Despite this, however, because Employee 2 did not click “Yes” in the dialog box when selecting the results of patient index searches, the user activity logs provided no information on which patients’ personal health information Employee 2 had used and disclosed in contravention of the *Act*.

At the time of both breaches, the Hospital’s Meditech system did not have the ability to record the selection of patient names on the patient index list. Simply put, the Hospital’s Meditech system did not provide that functionality despite the fact that by selecting a patient’s name on the patient index, the Employees were able to view demographic and personal health information about the patient including information relating to the dates of visits to the Hospital and health number. Thus, the Hospital rightly points to a “gap” in the capabilities of its Meditech system when explaining why, at the time of the second reported breach, it continued to lack information regarding the affected patients and therefore was not able to identify them for purposes of the notification required under section 12(2) of the *Act*.

Having said that, it is important to note that the Employees had similar duties and responsibilities with similar access rights to the Meditech system in both breaches — they were both in clerical positions with access to the entire patient index through the scheduling module of the Hospital’s Meditech system. However, according to the Hospital, it was only *after* the second

reported breach that it discovered this deficiency in its audit functionality.

In my view, this was too late. The Hospital should have come to this realization during its initial investigation into the first breach. The Hospital concluded that Employee 1 was using the personal health information about new mothers in contravention of the *Act*. In addition, the Hospital *knew* that Employee 1 was able to perform patient index searches and that selecting a patient name on the patient index would reveal personal health information about that patient. The Hospital confirmed this was the case in its letter to the IPC dated October 8, 2013, where it stated that the Hospital:

[e]stablished that the employee had access to schedule information which allowed him to view contact information (telephone and address) of expecting mothers *without accessing the patient record*. [Emphasis added]

On the basis of this information alone, the Hospital should have taken further steps to ensure that sufficient information about user activities within the scheduling module of its Meditech system was being captured in its user activity logs in the fall of 2013, if not sooner. With this critical information, it then could have put additional measures or safeguards in place, which may have mitigated the harm arising from the second breach. Why the Hospital did not carry through with a full assessment of its auditing capabilities in 2013, given the information available to it, is not clear to me.

In its representations, the Hospital stated that it did not know how Employee 1 accessed personal health information for the purpose of selling RESPs. I accept that the Hospital may not have had specific details of the manner in which Employee 1 accessed the personal health information of patients. However, statements from the Hospital in its letter of October 8, 2013 show that, at the very least, the Hospital knew what options were open to Employee 1 for accessing the personal health information of patients.

As noted above, to comply with section 12(1) of the *Act*, health information custodians must review from time to time the measures or safeguards that they have implemented to ensure that they continue to be “reasonable in the circumstances.” After the discovery of a contravention of the *Act*, such a review is absolutely essential. A health information custodian must conduct a thorough review to identify limitations or “gaps” in the measures or safeguards directly related to the contravention of the *Act* and address these limitations or “gaps” in a timely manner so as to prevent similar contraventions in the future.

In my view, the Hospital did not undertake a thorough enough review of its safeguards upon discovery of the first breach and so failed to introduce reasonable measures or safeguards in advance of the second breach that could have mitigated the harm and facilitated the identification of affected patients. As such, I find that the Hospital did not have measures or safeguards in place that were reasonable in the circumstances at the time of the second breach with respect to the information contained in its user activity logs.

According to the Hospital, it has been working with Meditech since the discovery of the second

breach to enhance the logging functionality of its auditing system. The Hospital submits that Meditech has provided it with a custom auditing feature that would log the selection of a patient name on the patient index. The Hospital has tested this feature and authorized its migration to the Hospital's Meditech system; however, I understand that the feature will not be available for use at the Hospital until the migration is accepted by the Hosting Provider.

In the Order provisions below, I will require the Hospital to implement this custom auditing feature in its Meditech system. In addition, I will require the Hospital to implement any other measures necessary to ensure that the Hospital is able to audit **all** instances where agents access personal health information in its Meditech system and in any other electronic information systems it uses, including the selection of a patient name on the patient index.

Search Controls

As noted in the background section of this Order, Employee 2 accessed the personal health information about new mothers by selecting their names or the names of their newborns from the results of a patient index search. To perform a patient index search in the Hospital's Meditech system, one must enter certain search criteria, for example, the patient's name and date of birth. The printouts of Meditech screen shots found in the second reported breach show that Employee 2 was able to return a list of newborns by searching for a patient with the name "AA" and a recent date of birth. When the term "AA" did not match any patients in the patient index, the Meditech system relaxed the search criteria and searched for any patients with the specified date of birth only. In this way, an open-ended search for newborns was performed by Employee 2 and by selecting the name of a newborn from the results of the search, Employee 2 was able to access information about the newborn's mother.

Another way to retrieve a list of newborns from patient index searches, and as a result gain access to personal health information about new mothers, is to search for a patient with the name "baby." Because the Hospital may not be aware of a newborn's given name until sometime after the birth, the newborn's record of personal health information will often initially list the newborn's first name as "baby girl" or "baby boy." Because of this, if an agent of the Hospital searches for a patient with the name "baby," and specifies a gender or date of birth, the system will return a list of newborns as matches.

A third way to retrieve a list of newborns from the patient index searches involves the fact that, according to the Hospital, the Meditech system defaults to a search for "baby" when the search criteria do not match any patient. In other words, one does not need to actually search for the name "baby" for results with that name to show up. The Hospital explained that when performing a search using a combination of name with gender or date of birth, the search algorithm works as a series of steps in which at each step, if a match is not found, the search criteria are relaxed from specific to more general and the search is performed again. As a final step, if the algorithm finds no approximate matches on the name, gender or date of birth entered, it "searches for the last name, 'BABY'."

The result of these three search configurations is that one does not need to know the name, address, health number or any other identifiable information about a particular patient to produce a list of newborns and their parents' contact details within the scheduling module of the Hospital's Meditech system through its search functionality.

The Hospital explained that its Meditech system does not have built-in functionality to limit the ability of agents of the Hospital to perform open-ended searches of the nature used by Employee 2. According to the Hospital, "[t]he search algorithm for the patient index is standard Meditech functionality" and "[t]he number of search results is not customizable."

Accordingly, at the time of the breaches, the Hospital did not have any search controls in place. The Hospital submits that, since this review was commenced, it has requested Meditech to remove the search term "baby" from its search algorithm as a possible future safeguard. This would prevent a list of newborns from being returned if the Meditech search algorithm finds no exact or approximate matches for the other search criteria. The Hospital has indicated that it does not know when Meditech will provide this functionality.

However, I note that this is only one of the ways of retrieving a list of newborns through the Hospital's search system. It would not affect the ability of agents to retrieve a list of newborns by searching for a patient with a meaningless name — e.g., "AA"— and a recent date of birth, nor would it prevent agents from searching for patients with the name "baby."

Another approach available to the Hospital is to look at ways in which agents use the Meditech system for authorized purposes and restrict the system's functionality to only those uses. The Hospital explained that in addition to partial first or last name plus date of birth or gender, patient index searches can be initiated by any of the following criteria:

1. health number;
2. medical record number (MRN);
3. encounter number; or
4. exact first name, last name and date of birth.

What is important to note about these searches is that in contrast to open-ended searches where a list of patients who partially match the criteria is returned, these would only return a single patient, if there was in fact a match, for the majority of cases.

If the Hospital's Meditech system had been configured to allow only these four types of searches, the occurrence of both reported breaches may have largely, if not entirely, been prevented. Since open-ended searches that return lists of patients who partially match the search criteria would not have been allowed, the Employees would not have been able to go "fishing" for information about new mothers.

The Hospital states that disallowing open-ended searches that return lists of patients who partially match the search criteria would adversely affect the ability of agents to schedule ap-

pointments and procedures for patients. According to the Hospital, the ability to relax search criteria from specific to more general is necessary for the following reasons:

(a) the patient name may not be always spelled correctly (long names are particularly challenging); (b) the patient name may be spelled phonetically; (c) common names or very short names may produce hundreds of matches in which case, additional search criteria such as gender or date of birth are required to narrow the search.

With respect to (a) and (b), if the Hospital's Meditech system were configured to allow only four types of searches, namely health number, MRN, encounter number, or exact first name, last name and date of birth, then agents would still be able to find patients on the patient index list with misspelled names or phonetically spelled names by using one of the other allowable search criteria.

With respect to (c), I do not see how this demonstrates a need for open-ended searches. Rather than a case where search criteria are relaxed, it describes a case where search criteria are *further restricted*. As such, it is not an argument for open-ended searches, but rather an argument *against* them.

For these reasons, I do not find the Hospital's arguments convincing. Disallowing open-ended searches that return lists of patients who partially match the search criteria would *not* adversely affect the ability of agents to perform their duties and are measures that are reasonable in the circumstances to ensure that personal health information is protected against unauthorized use or disclosure. The Hospital should have asked Meditech to address this shortcoming in the Meditech system or should have looked at other technical solutions if not after the first reported breach, then definitely after the second.

In the Order provisions below, I will require that the Hospital work with Meditech or another software provider to develop a solution that will limit the ability of its agents to perform open-ended searches for personal health information about patients in accordance with the comments above.

Administrative Measures or Safeguards

In order to comply with the requirement in section 12(1) of the *Act* to take steps that are reasonable in the circumstances to protect personal health information, health information custodians must implement administrative measures or safeguards, including privacy policies, procedures and practices, as well as privacy training and awareness programs and initiatives. Comprehensive privacy policies, procedures and practices, as well as comprehensive privacy training, are critical in protecting personal health information from unauthorized use and disclosure and from other contraventions of the *Act*. This is particularly important in relation to electronic information systems which provide agents with the ability to access a vast amount of personal health information.

The Hospital states that, in addition to the technological measures or safeguards in place, it has implemented a number of administrative measures or safeguards to protect personal health information. It provided the IPC with policies, procedures and practices to support its position.

The Hospital also states that following the first breach it understood that it needed to implement more frequent privacy training and that “it is considering additional means it can use to reinforce its culture of privacy.” It adds that the administrative measures or safeguards it has implemented are reasonable in the circumstances as measured against Ontario health sector practices and more specifically the practices of similarly situated public hospitals, but it provides no information or evidence to support this claim. Even if it had provided more information or evidence, these factors would not be determinative of the question whether the hospital has complied with its obligations under section 12(1).

I have reviewed all of the policies, procedures and practices provided by the Hospital. In the discussion that follows, I comment on a number of those policies, practices and procedures. I also find that the Hospital has not developed some policies, practices and procedures which it should have developed in order to meet its obligations under section 12(1) of the *Act*.

Privacy Audits Policy

The *Privacy Audits* policy was revised in May 2009. Its stated purpose is to ensure that the Hospital’s “clinical information computer systems” have “regular audits and any findings of non-compliance with privacy policies [of the Hospital] and/or legislation are investigated by the Manager or Chief of Program.” The *Privacy Audits* policy also provides that the Privacy Coordinator is responsible for conducting “audits on a random basis to review access by staff, physicians or volunteers, with the same last name as a patient, next of kin, person to notify, guarantor or RVHS employer, in the Master Patient Index.” The policy also sets out the steps that will be taken by the Privacy Coordinator following an audit if it is determined that further investigation is required.

In the Notice of Review sent to the Hospital, I asked it to provide information concerning the audits it conducted, the frequency with which and the circumstances in which audits are conducted, the process that is followed in conducting the audits, the number and nature of the records of personal health information audited and how the findings of any such audits are addressed.

In response, the Hospital stated:

In the past, the Hospital audited user activity on request and following a suspected incident. In October 2013, the Hospital intensified its auditing program and in June 2014, introduced weekly random audits. [Emphasis added.]

Since user-based auditing is not highly effective in identifying inappropriate ac-

cess, the Hospital created data mining programs to look for unusual access patterns. These programs identify suspicious access which the Hospital investigates with applicable users.

The *Privacy Audits* policy requires the conduct of “random audits.” Random audits are restricted to a review of access “by staff, physicians or volunteers, with the same last name as a patient, next of kin, person to notify, guarantor or RVHS employer in the Master Patient Index.” These types of audits are important but by themselves insufficient. The Hospital must conduct random audits on all users’ activities and it must also conduct random audits of the records of personal health information of high profile individuals.

The Hospital must also implement measures to ensure it is able to conduct random audits on **all** activities in its electronic information systems and these measures must be reflected in the *Privacy Audits* policy. The Hospital’s failure to ensure that it has the ability to conduct random audits on all uses of the scheduling module and its failure to conduct random audits are a contravention of section 12(1) of the *Act*.

I am equally concerned that the Hospital was **not** following its own *Privacy Audits* policy because it was only conducting audits in response to requests and following “a suspected incident” despite the requirement to conduct random audits. In my view, reactive auditing is inadequate and does not meet the Hospital’s obligations pursuant to section 12(1) of the *Act* and is contrary to the Hospital’s own policy.

My other concern with the *Privacy Audits* policy is that, although it sets out the steps the Hospital must take if a privacy breach is suspected, it does not set out what actions must be taken if a breach is identified. I will discuss this further in the context of my discussion about the Hospital’s obligations under section 10 of the *Act*, which appears later in this Order.

Having found that the Hospital contravened section 12(1), and in view of the Hospital’s lack of awareness about the limitations in the auditing functionality of the Meditech system, in the Order provisions below, I will require the Hospital to review and revise its *Privacy Audits* policy to require that measures be implemented to ensure that the activities of all agents on all of its electronic information systems can be audited. The policy must also require that audits be conducted on request, following the report of an actual or suspected privacy breach and on a random basis. In addition, in relation to high profile patients, audits must be conducted frequently.

Privacy Training Program Policy

At the time of the two reported breaches, the Hospital’s practice was to conduct privacy training during the orientation of new employees. It also conducted training in 2004 when the *Act* was proclaimed in force. With respect to the training program, the Hospital provided the IPC with a copy of its general orientation program, its “2004 PHIPA rollout” document and a copy of a PowerPoint presentation on the *Act*.

In its representations, the Hospital acknowledged that it needs to implement more frequent privacy training and that it was investigating options for delivering supplemental “refresher” training when it learned that Employee 2 was using and disclosing personal health information in contravention of the *Act*. It also stated that:

In July of 2014, as an interim step, the Hospital conducted two privacy education sessions, one in a leadership forum attended by managers and one in a town hall for staff. The Hospital intends to implement on-line privacy modules for employees to complete on an annual basis, or more frequently if recommended by their manager. The Hospital is consulting with the Ontario Hospital Association about available on-line privacy training programs to expedite the implementation of this type of privacy training for all staff members.

I note that in September 2014, approximately one year after the first breach was reported to the IPC, the Hospital stated that it was consulting with the Ontario Hospital Association (OHA) regarding the availability of on-line training programs. I am aware that the OHA has an on-line training resource that deals specifically with the issue of unauthorized access to personal health information by agents. Steps should have been taken by the Hospital much earlier to ensure that all agents of the Hospital were provided with this type of training.

In addition, the Hospital does not record whether or not agents attend privacy training and therefore was unable to confirm that Employee 1 and Employee 2 had received any privacy training when they were initially hired by the Hospital. The Hospital must take steps to ensure that attendance at privacy training is documented.

A comprehensive privacy training program is an essential tool to combat the risk of uses and disclosures of personal health information by agents in contravention of the *Act*, including agents who are “curious” or who are motivated by their own interests, such as financial gain. The training program must be detailed in a *Privacy Training Program* policy. The *Privacy Training Program* policy must require agents to complete privacy training upon the commencement of their employment, contractual or other relationship with the Hospital and before they are given access to personal health information in the custody or control of the Hospital. The *Privacy Training Program* policy must further require that agents complete privacy training annually. It must also clearly define who is responsible for developing the privacy training materials and for providing the training. Further, it must require that the attendance of agents at the initial and annual privacy training be documented and must identify the person(s) responsible for documenting attendance, for identifying agents who do not attend such training and for ensuring that such training is completed. It must also require that the privacy training materials be reviewed and updated on a regular basis to address:

Any orders, guidelines, fact sheets and best practices issued by the IPC under the *Act*;

Evolving industry standards and best practices;

The implementation of new technologies, programs or services;

Amendments to the *Act*,

New or amendments to privacy policies, procedures or practices implemented by the Hospital;
and

Recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches.

In the Order provisions below, I will require the Hospital to develop and implement a *Privacy Training Program* policy in accordance with the comments above.

Privacy Training Materials

The Hospital's training materials contain information about the *Act* and best practices. However, this training material lacks detail in some areas and essential information. The training materials must be amended to include detailed information in relation to the following:

- the purposes for which agents of the Hospital are permitted to collect, use and disclose personal health information and any limitations imposed by the Hospital;
- the privacy policies, procedures and practices implemented by the Hospital and the obligations imposed on agents by these policies, procedures and practices;
- the obligations of agents under the *Act*, including the duty to notify the Hospital at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons and the procedure for doing so;
- the potential consequences that may be imposed on agents who collect, use or disclose personal health information in contravention of the *Act* and/or the privacy policies, procedures and practices implemented by the Hospital;
- the potential consequences for the Hospital arising from agents who collect, use or disclose personal health information in contravention of the *Act*;
- the circumstances surrounding the contraventions of the *Act* by Employee 1 and Employee 2, including the findings made in this Order regarding these contraventions, and the consequences of these contraventions for the Hospital and the employees involved.

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. In the Order provisions that follow, I will require that the Hospital review and revise its privacy training materials in accordance with the comments above.

Privacy Awareness Programs and Policies

The development of a culture of privacy within any organization is also dependent on the level of awareness beyond training. When asked to describe any steps that the Hospital has taken to foster a culture of privacy and raise awareness among agents of their duties under the *Act* and of their duties under the privacy policies, procedures and practices implemented by the Hospital, the Hospital responded as follows:

Privacy awareness is fostered through means that include “e-Echo mail blasts” which are a form of internal electronic bulletin. In the past, there would typically be at least one article per year on a privacy-related matter. An alert reminding users of the restrictions on access pops up when a user logs on to Meditech.

The Hospital is considering additional means it can use to reinforce its culture of privacy including the use of posters and annual attestations by employees that they are not engaged in activities outside of the Hospital that place them in a conflict of interest with their obligations to the Hospital. The Hospital is cognizant of its obligations under labour and employment laws and is working with its HR department in this regard: it has found enforcement more of a challenge in its unionized environment than privacy awareness.

I am satisfied that the Hospital is considering additional communications tools to assist it in complying with section 12(1). However, more than one year has passed since the first reported breach which is more than sufficient time to develop and implement measures such as these. As such, the Hospital must review its current communications practices to ensure that they are promoting and fostering a strong culture of privacy and it must develop a *Privacy Awareness Program* policy. The policy must require the development of a communications program to frequently remind agents of the privacy and security policies, procedures and practices implemented by the Hospital and of the obligations imposed on agents by these policies, procedures and practices, as well as their obligations under the *Act*. It must also identify the individual responsible for implementing the *Privacy Awareness Program* and set out the frequency, method and nature of the privacy awareness communications to be delivered to all agents.

In the Order provisions below, I will require the Hospital to develop and implement a *Privacy Awareness Program* policy in accordance with the comments above.

Pledge of Confidentiality policy

The Hospital submits that its “new employees and others, including temporary employees and volunteers” are required to sign a “Pledge of Confidentiality” when they are hired as well as “at other points in the employment relationship.” This requirement is set out in a *Pledge of Confidentiality* policy.

The Hospital did not explain what it meant by the words “at other points in the employment re-

lationship.” However, the Hospital confirmed that both Employees signed a “Pledge of Confidentiality” upon hiring. Employee 2 was also required to re-execute the “Pledge of Confidentiality” following a gap in her employment.

By signing this pledge, these two Employees acknowledged that they understood that they were prohibited from accessing patient information “without authorization to do so and without a ‘need-to-know’ basis for direct patient care or the performance of one’s duties.”

The Hospital must clarify that the Hospital’s *Pledge of Confidentiality* policy and the “Pledge of Confidentiality” apply to all agents, not just employees of the Hospital. It must also:

- require agents to comply with the *Act* and its regulations;

- require agents to securely return all property of the Hospital including keys and records of personal health information, if any, at the conclusion of their employment or contractual or other relationship; and

- require agents to notify the Hospital at the first reasonable opportunity in accordance with the Hospital’s *Privacy Breach Management* policy, if they believe that there may have been a breach of the “Pledge of Confidentiality” or if the agent breaches or believes there may have been a breach of privacy policies, procedures and practices implemented by the Hospital, or a breach of the *Act*.

The *Pledge of Confidentiality* policy states that breaches of the “Pledge of Confidentiality” will result in discipline up to and including termination of employment or hospital privileges and/or hospital affiliation as applicable. This must be amended to clarify that a breach may also result in the termination of a contractual relationship and a report to the agents’ health regulatory college, where applicable.

Unfortunately, the policy also states “[r]andom audits may be carried out to ensure compliance with this policy.” The *Pledge of Confidentiality* policy must be amended to read that the Hospital *will* conduct random audits in order to ensure that agents are deterred from using or disclosing personal health information in the Hospital’s electronic information systems in contravention of the *Act*.

In addition, the Hospital’s current practice of having employees sign the pledge upon hiring is not sufficient. All agents of the Hospital must be reminded annually of their obligations under the *Act* and under the privacy policies, procedures and practices implemented by the Hospital. A “Pledge of Confidentiality” is one of the many administrative measures open to the Hospital to do this. To be effective, a “Pledge of Confidentiality” must be signed by all agents on an annual basis. The Hospital’s failure to adopt this practice is a shortcoming in its current administrative measures and safeguards. The Hospital must ensure that all agents of the Hospital sign the “Pledge of Confidentiality” and that it be signed at the commencement of an agent’s employment, contractual or other relationship with the Hospital and then on an annual basis.

In the Order provisions that follow, I will require the Hospital to review and revise its *Pledge of*

Confidentiality policy and “Pledge of Confidentiality” in accordance with the comments and findings made above.

Privacy Advisory

The Hospital states that when an agent logs on to the Meditech system, an alert appears on the login screen reminding him or her of the restrictions on access. The alert states:

PRIVACY ADVISORY

This system contains personal information about our patients and staff. Access to this information is permitted for patient care purposes and/or for the performance of your work duties. Access to information in this system is audited regularly. Inappropriate access may result in suspension or termination of your access privileges and disciplinary action up to and including termination of employment or affiliation.

Privacy and Confidentiality Policies must be reviewed and understood before entering this system.

Notices alerting agents of the consequences of using or disclosing personal health information in contravention of the *Act*, such as this *Privacy Advisory*, can be effective tools for protecting privacy.²² However, this *Privacy Advisory* lacks essential features.

The *Privacy Advisory* must be amended to clarify that the use or disclosure of personal health information in the system is permitted “**only**” for the purposes of providing health care to the patient and/or in the performance of the agent’s duties. The *Privacy Advisory* must also appear on its own screen and it must require the agent to acknowledge that he or she has read, understood and agrees to comply with these terms and with the privacy policies, procedures and practices of the Hospital prior to permitting the agent or user to access the Hospital’s electronic information systems. In the Order provisions below, I will require the Hospital to review and revise the *Privacy Advisory* in accordance with the comments and findings above.

Issue F: Did the Hospital have in place information practices that

²² Order HO-010, *supra* note 2.

comply with the Act and did it comply with its information practices in accordance with section 10(1) and 10(2) of the Act?

Section 10(1) of the *Act* states:

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.

Section 10(2) of the *Act* states:

A health information custodian shall comply with its information practices.

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.

Health information custodians must review their information practices on an ongoing basis to ensure that they are current and take into account: evolving industry standards and best practices; new technologies, programs or services; any orders, guidelines, fact sheets and best practices issued by the IPC under the *Act*; amendments to the *Act*; and recommendations arising from privacy audits, privacy impact assessments and investigations into privacy complaints and privacy breaches. It is also important for health information custodians to review their information practices on an ongoing basis to ensure their information practices, as set out in privacy policies and procedures, continue to be consistent with their actual practices.

In Order HO-004, the IPC stated:

Health information custodians should review their information practices regularly to ensure that they remain appropriate for their operations. As the health information custodian’s operations evolve and grow, and as a result of the introduction of new information technology, it is important to update information practices to reflect these changes. A health information custodian should take steps to ensure that the contents of its policies and procedures are kept current to reflect actual practices. In addition, a health information custodian should keep abreast

of developments relating to safeguards to ensure that they comply with the *Act*.

In addition, when adopting policies and procedures, a health information custodian needs to ensure that staff members and independent contractors are made aware of new policies and procedures by proper notice, either through the use of internal mail system, electronic mail and/or educational sessions.

Privacy policies and procedures on their own, however, are not sufficient. Health information custodians must also take steps to ensure that agents are aware of and understand their obligations and limitations under the *Act* and under the privacy policies, practices and procedures that custodians have implemented and that agents are aware of and understand the consequences of failing to comply with these obligations and limitations.

In its written representations, the Hospital takes the position that its information practices complied with sections 10(1) and (2) of the *Act* and restates its position that the issue in this review is that the Employees did not comply with the Hospital's information practices.

I reviewed the relevant Hospital's policies, procedures and practices in the preceding discussion and found that they did not meet the Hospital's obligations under section 12(1) of the *Act*. For the same reasons, I find that these same policies, practices and procedures do not comply with the requirements of section 10(1) of the *Act*.

In addition, as I mentioned above, the Hospital has not developed a *Privacy Breach Management* policy and in the Order provisions below I require the Hospital to do so. A *Privacy Breach Management* policy is necessary to ensure the proper identification, reporting, containment, notification, investigation and remediation of privacy breaches, including contraventions of the *Act*, and that agents understand their duties and responsibilities in this regard. The policy must include a requirement that a review be conducted following a breach to ensure that steps are taken to prevent further unauthorized use or disclosure of personal health information, by identifying any risks and taking steps to mitigate those risks.

If a policy, practice or procedure had been in place requiring a complete review of the Hospital's Meditech system as a result of the first reported breach, the Hospital may have identified the limitations or gaps in its auditing program and in its *Privacy Audits* policy, and taken steps to address these limitations or gaps before the second breach. If it had done so, the Hospital may have been in a position to prevent some of the unauthorized uses and disclosures by Employee 2 and would have been able to identify patients whose personal health information was used and disclosed by Employee 2 in contravention of the *Act* in the period of time between the first and the second reported breach.

As a result, the Hospital must develop a *Privacy Breach Management* policy that:

- a) Imposes an obligation on agents to notify the Hospital if personal health information is stolen, lost or accessed by unauthorized persons and identifies who at the Hospital must be notified and the time frame for notification;

- b) Mandates that agents report a breach to senior management, and sets out who is responsible for such reporting, the time frame within which this reporting must be completed and to whom it must be reported;
- c) Sets out the circumstances in which a privacy breach should be reported to others including police, health regulatory colleges and the IPC;
- d) Requires immediate measures be taken to contain the breach to ensure that steps are taken that are reasonable in the circumstances to protect personal health information from further theft, loss or unauthorized use or disclosure and to protect records of personal health information from further unauthorized copying, modification or disposal;
- e) Requires notification of the affected individual(s) pursuant to the *Act*, and sets out who is responsible for providing notification and the information to be provided;
- f) Requires that an investigation of the breach be conducted including a review of all relevant information systems and policies, practices and procedures;
- g) Sets out who is responsible for investigating, the nature and scope of the investigation and the process to be followed in the investigation; and
- h) Sets out the process by which the findings of the investigation, including any recommendations are communicated and implemented and the person responsible for implementation.

As noted above, in relation to its *Privacy Audits* policy, the Hospital stated:

In the past, the Hospital audited user activity on request and following a suspected incident. In October 2013, the Hospital intensified its auditing program and in June 2014, introduced weekly random audits. [Emphasis added.]

Given that the *Privacy Audits* policy requires the conduct of “random audits,” the Hospital’s practice of conducting audits on request and following a breach amounts to a failure to comply with its own policies contrary to section 10(2) of the *Act*. The Hospital must take steps to ensure that it complies with its *Privacy Audits* policy.

In the Order provisions below, I will require that the Hospital develop a *Privacy Breach Management* policy in accordance with the comments and findings above and that it take steps to ensure that it complies with the *Privacy Audits* policy.

SUMMARY OF FINDINGS

I have made the following findings in this review:

1. The information at issue in this review is “personal health information” as defined in sec-

tion 4 of the *Act*.

2. The Hospital is a “person” who operates a hospital within the meaning of the *Public Hospitals Act* and it is a health information custodian with custody or control of the personal health information at issue as defined in section 3(1)4i of the *Act*.
3. Employee 1 and Employee 2 were agents of the Hospital as defined in section 2 of the *Act*.
4. The personal health information at issue in this review was used and/or disclosed in contravention of the *Act*.
5. The Hospital did not take steps that are reasonable in the circumstances to ensure that personal health information in its custody or control is protected against unauthorized use or disclosure in contravention of section 12(1) of the *Act*.
6. The Hospital did not have information practices that comply with the *Act* and did not comply with its information practices, in contravention of sections 10(1) and 10(2) of the *Act*.

ORDER

I order the Hospital to:

1. In relation to all of the Hospital’s electronic information systems, implement the measures necessary to ensure that the Hospital is able to audit all instances where agents access personal health information on its electronic information systems, including the selection of patient names on the patient index of its Meditech system.
2. In relation to the Hospital’s Meditech system:
 - a) Work with the Hospital’s Hosting Provider to review and amend the service level agreement between the Hospital and the Hosting Provider to clarify the responsibility for the creation, maintenance and archiving of user activity logs generated by the Hospital’s use of its Meditech system, and ensure that the user activity logs are available to the Hospital for audit purposes.
 - b) Work with Meditech or another software provider to develop a solution that will limit the search capabilities and search functionalities of the Hospital’s Meditech system so that agents are unable to perform open-ended searches for personal health information about individuals, including newborns and/or their mothers, and can only perform searches based on the following criteria: health number, medical record number, encounter number, or exact first name, last name and date of birth.
3. Review and revise its *Privacy Audits* policy, the *Pledge of Confidentiality* policy and the

“Pledge of Confidentiality,” and the *Privacy Advisory* in accordance with the comments and findings made in this Order, and take steps to ensure that it complies with the *Privacy Audits* policy.

4. Develop and implement a *Privacy Training Program* policy, a *Privacy Awareness Program* policy, and a *Privacy Breach Management* policy in accordance with the comments and findings made in this Order.
5. **Immediately** review and revise its privacy training tools and materials in accordance with the comments and findings made in this Order.
6. Using the privacy training materials developed in accordance with Order provision 5:
 - a) **immediately** conduct privacy training for all agents in clerical positions in the Hospital; and
 - b) conduct privacy training for all other agents by **June 16, 2015**.
7. Provide this office with proof of compliance with all of the Order provisions by **September 16, 2015**.

Signed by Brian Beamish. December 16, 2014.

POSTSCRIPT

The *Personal Health Information Protection Act, 2004* (the *Act*) was enacted 10 years ago, on November 1, 2004, to establish rules governing the collection, use and disclosure of personal health information within the health sector. Over the last decade, this office has seen a growing number of privacy breaches involving unauthorized use, often described as unauthorized access, to personal health information by employees, staff and other agents of health information custodians. Indeed, while this review was underway, three additional cases of unauthorized access were reported in the media.

Efforts to combat this issue require action by multiple stakeholders. Health regulatory colleges have a role to play where regulated health professionals breach standards of professional conduct. Health information custodians, such as hospitals, must also ensure that staff are fully aware of their duties and obligations to protect the privacy of patients and the confidentiality of their personal health information. As this Order makes clear, custodians have an important role in auditing access to electronic health records and taking appropriate disciplinary and other actions when unauthorized access is detected. Full disclosure of the actions taken in response to a breach, including the disciplinary actions taken against staff, may assist in deterring other

similar conduct and will demonstrate a commitment to transparency and accountability.

Part of this office's role is to investigate and review instances of unauthorized access to ensure that health information custodians are meeting their responsibilities by implementing proper privacy policies, practices and procedures; conducting staff training; monitoring access to health records; and implementing technical, physical and administrative safeguards to protect the privacy of patients.

There are measures in the *Act* designed to promote greater accountability that are not being used to the extent that they should. Section 72(1)(a) of the *Act* states that a person is guilty of an offence if the person "wilfully collects, uses or discloses personal health information in contravention of this Act or its regulations." Individuals found guilty of an offence under this section are liable, on conviction, to a fine of up to \$50,000. No person other than the Attorney General or his agent may commence a prosecution for an offence under the *Act*.

The fact that charges might be laid should be a significant deterrent to agents, but the prospect of charges will only have that effect if health information custodians and their agents know that this provision is likely to be used in appropriate cases.

Since the *Act* was passed 10 years ago, charges under section 72(1)(a) of the *Act* have been laid in only one case, and that case is still pending before the courts. More needs to be done to address what appears to be a growing problem. To that end, we have initiated discussions with the Ministry of Health and Long-Term Care and the Ministry of the Attorney General with a view to developing a protocol for the Attorney General to commence prosecutions in appropriate cases.

The Legislature clearly contemplated that there would be serious consequences for failure to comply with the *Act* — it is time to make use of all the tools available to send a strong message to health information custodians and their agents that breaches of this kind will not be tolerated.