Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 64

HR15-115

A Public Hospital

December 18, 2017

Summary: A public hospital (the hospital) contacted the Office of the Information and Privacy Commissioner of Ontario (the IPC) to report a privacy breach under the *Personal Health Information Protection Act, 2004* (*PHIPA*). This breach involved a registration clerk (the employee) accessing records of personal health information relating to a media-attracting patient (the patient) as well as 443 other patients, without authorization. The IPC referred this matter to the Attorney General of Ontario to consider commencing a prosecution against the employee for offences under *PHIPA*. A prosecution was subsequently commenced and the employee pled guilty. As part of her plea, the employee agreed that she wilfully used personal health information in contravention of *PHIPA*. In light of the steps taken by the hospital to address this breach, including its acknowledgement of the benefits and importance of including enhanced auditing capabilities in any new system it implements, no review of this matter will be conducted under Part VI of *PHIPA*.

Statutes considered: *Personal Health Information Protection Act, 2004*, sections 2, 12(1), and 29.

BACKGROUND:

[1] A public hospital (the hospital) contacted the Office of the Information and Privacy Commissioner of Ontario (the IPC) to report a privacy breach under the *Personal Health Information Protection Act, 2004* (*PHIPA*). This breach involved a registration clerk (the employee) accessing records of personal health information relating to a media-attracting patient (the patient) as well as 443 other patients,

without authorization.

[2] The hospital explained to the IPC that it first became aware of this privacy breach when, in accordance with the hospital's protocol for media-attracting patients, a staff member in its privacy office performed an audit of its electronic health records system to determine who had accessed the records of the patient. As is common practice for hospitals in Ontario, the hospital uses an electronic health records system to facilitate the provision of health care to its patients.

[3] The audit of the hospital's electronic health records system showed that the employee had accessed the media-attracting patient's medical records. The hospital interviewed the employee to ask about her reason for accessing the media-attracting patient's health records. The employee was unable to provide the hospital with a satisfactory response regarding why she had accessed the patient's personal health information.

[4] Upon learning of the breach, the hospital initiated an internal investigation, which included an audit of the employee's access to the electronic health records system for the year leading up to this breach. The audit uncovered that the employee had inappropriately accessed the medical records of 443 other patients.

[5] According to the hospital, the types of medical information that its employees have access to through its electronic health records system is role-based – that is, employees are only provided with as much information as is required to perform their employment duties. In this case, the employee was a registration clerk and only had access to a limited amount of medical information – specifically, patients' names, hospital numbers, addresses, telephone numbers, sex, dates of birth, history of hospital visits, and the diagnosis at the time of their admissions.

[6] The hospital explained to the IPC that the auditing capability of its current electronic health records system is limited to identifying which system user has accessed a patient record, and is not able to detect which types of medical records have been accessed. As previously noted, in this case, because the employee in question was a registration clerk, the amount and type of patient information that she had access to, albeit sensitive in nature, was limited in scope.

[7] As part of the hospital's strategy in containing the privacy breach, as soon as it became aware of it, the employee was suspended from her position at the hospital and her access to the hospital's electronic health records system was revoked.

[8] Once the hospital was able to conduct internal interviews and a preliminary investigation, the employee was discharged. At that time, the employee's hospital keys, pager and hospital ID badge were all returned to the hospital.

[9] The IPC referred this matter to the Attorney General of Ontario to consider commencing a prosecution against the employee for offences under *PHIPA*. A

prosecution was subsequently commenced and the employee pled guilty. As part of her plea, the employee agreed that she wilfully used personal health information in contravention of *PHIPA*.

DISCUSSION:

[10] There is no dispute that the hospital is a "health information custodian" and that the hospital records accessed by the employee contained "personal health information" under *PHIPA*.

[11] Based on the information set out above, as a preliminary matter, I find that the hospital is a "health information custodian" under paragraph 4.i of section 3(1) of *PHIPA*, and that the records at issue are "personal health information" under sections 4(1)(a) and (b) of *PHIPA,* which were in the custody or control of the hospital. There is no dispute, and I further find, that the employee was an "agent" of the hospital, as that term is defined in section 2 of *PHIPA.*

ISSUES:

[12] In this decision, the following issues will be discussed:

1. Was personal health information "used" and/or "disclosed" in compliance with *PHIPA*?

2. Did the hospital take steps that were reasonable in the circumstances to protect personal health information in accordance with section 12(1) of *PHIPA*?

RESULTS OF THE INVESTIGATION:

Issue 1: Was personal health information "used" and/or "disclosed" in compliance with *PHIPA*?

[13] Section 2 of *PHIPA* 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.[1]

[1] This is the definition of "use" in force at the time of these events. The definition of use has since been amended to clarify that viewing personal health information is also a use.

> "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;

[14] Under *PHIPA*, personal health information is permitted to be used or disclosed with consent, or if the use or disclosure is otherwise permitted or required by that *Act.* Section 29 of *PHIPA* states:

> **Requirement for consent**
>
> 29. A health information custodian shall not collect, use or disclose personal health information about an individual unless,
>
> > (a) it has the individual's consent under this *Act* and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or
> >
> > (b) the collection, use or disclosure, as the case may be, is permitted or required by this *Act*.

[15] In its interview with the employee upon learning of the breach, the hospital specifically asked the employee why she had accessed the media-attracting patient's personal health information. The employee was unable to provide the hospital with an explanation for her actions.

Use of Personal Health Information

[16] I find that the employee's actions of accessing the personal health information of the media-attracting patient and the 443 other patients through the hospital's electronic health records system was a "use" within the meaning of section 2 of *PHIPA*. This is in keeping with the plain meaning of the phrase "to handle or deal with the information" in the definition of use, as quoted earlier in this decision.

[17] There is no information or evidence before me to suggest that the patients consented to this use of their personal health information or that the employee could

---

I further note that section 6(1) of *PHIPA* states that 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.

assume the patients' implied consent.[2]

[18] Section 37 of *PHIPA* sets out the purposes for which personal health information may be used without a patient's consent. I have not been provided with any information to suggest that the employee's use of the patients' personal health information was for a purpose set out in section 37 of *PHIPA*.

[19] The hospital has informed the IPC that this "use" of personal health information did not comply with *PHIPA*. In fact, as previously noted, as part of the employee's plea with the Ministry of the Attorney General in relation to the charges brought against her, the employee pled guilty to wilfully using individuals' personal health information in contravention of *PHIPA*.

[20] The hospital agrees, and I find, that the personal health information was used without the patients' consent and that this use was not permitted by section 37 of *PHIPA*. Accordingly, I find that the employee's use of the personal health information in these circumstances did not comply with *PHIPA*.

Disclosure of Personal Health Information

[21] During the hospital's interview with the employee upon learning of the breaches the hospital specifically asked the employee if she had disclosed patients' personal health information to any other person or health information custodian. The employee stated that she had not disclosed any patients' personal health information.

[22] There is no evidence before me to suggest that the employee disclosed the personal health information she accessed. For this reason, I do not find that the employee disclosed any personal health information in contravention of *PHIPA*.

Issue 2: Did the hospital take steps that were reasonable in the circumstances to protect personal health information in accordance with section 12(1) of *PHIPA*?

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

> **Security**
>
> 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

[2] See *PHIPA,* s. 20(2).

> unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

[24] The scale and circumstances of this privacy breach raised questions about whether the hospital was taking reasonable steps to ensure the security and privacy of personal health information, and prompted this investigation.

[25] In Orders HO-010 and HO-013, the IPC considered "reasonable" for the purposes of section 12(1) of *PHIPA*, to include a health information custodian reviewing, from time to time, the measures or safeguards it has in place 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.

[26] Under *PHIPA*, health information custodians are expected to identify 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.[3]

[27] As stated by Commissioner Brian Beamish in Order HO-013, "[a]s 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 [PHIPA], will also evolve."

[28] The issue of hospital agents accessing records of personal health information without authorization is one that has garnered a great deal of attention in recent years. Both the IPC and other privacy commissioners have issued several orders or reports where breaches of personal health information have occurred as a result of unauthorized access.

[29] In May 2016, the Ontario legislature passed health privacy legislation that, among other things, amended *PHIPA* to increase fines for offences under that *Act* and eliminated the six-month limitation period for commencing a prosecution for such offences. The amendments also included mandatory reporting of privacy breaches to the IPC in specific circumstances as prescribed in regulation. These mandatory notification requirements under *PHIPA* came into force on October 1, 2017.

As part of my investigation, I reviewed the technical and administrative safeguards used by the hospital to ensure the security and privacy of personal health information, and highlight the following.

---

[3] *PHIPA* Order HO-013.

Administrative Measures or Safeguards

Privacy Policies & Procedures

[30] The hospital has both a Privacy Breach Management Policy and a Privacy Breach Protocol – "Managing a PHI Breach".

[31] The Privacy Breach Management Policy defines important terms, such as "personal health information" and "privacy breach". It also includes practical, real-life examples of privacy breaches, including a lost or misplaced USB key containing personal health information; compromised passwords; or external hacker attacks.

[32] The Privacy Breach Management Policy includes, among other things, the following requirements:

1. All hospital agents must immediately report privacy breaches and suspected breaches to the hospital's privacy office, who may then – depending on the severity of the breach – notify senior management;

2. The privacy office will adhere to its Privacy Breach Management Protocol for breach management, which includes the following requirements:

    - Stopping and containing the breach;
    - Contacting the IPC of the breach, if appropriate;
    - Notifying affected individuals at the first reasonable opportunity if their personal health information has been breached; and
    - Conducting an investigation into how and why the breach occurred. Upon completion of the hospital's investigation, it then decides what remediation would be appropriate.

[33] Recently, the hospital's privacy-related policies have been revised to include more explicit detail on discipline as a result of privacy breaches, and all privacy training materials have been revised to align with this change. The hospital's privacy training program is described in more detail, below.

Confidentiality Agreements

[34] All hospital agents must sign a confidentiality agreement at the time of hire. Since this breach, the hospital has made changes requiring that all agents also sign a confidentiality agreement on an annual basis.

[35] The hospital's Confidentiality Agreement requires agents to acknowledge the privacy obligations and expectations, including the consequences of a privacy breach. It also requires agents to confirm that they have read and understand the conditions of

the hospital's agreement, as well as its policies on security, privacy, and confidentiality.

[36] The hospital's Confidentiality Agreement sets out the purposes for which agents are permitted to collect, use, and disclose personal health information, as well as any limitations, conditions or restrictions placed on the collection, use, and disclosure. It also advised that agents are told that the hospital may conduct periodic audits to ensure compliance and data integrity.

Privacy Warnings

[37] Upon logging onto the hospital's electronic health records system, hospital agents previously received the following warning:

> As an agent and user of our patient care system, you have an obligation to respect the privacy of all patients. Access to information is permitted by law, but only as it relates to the role you perform at the hospital.

[38] Since the breach, the hospital has revised the wording of its privacy warning to state:

> Accessing any patient information in the system is permitted ONLY for the purposes of providing health care to the patient and/or in the performance of your duties as an agent of the hospital. By proceeding further, you acknowledge that you have read, understand, and agree to comply with the terms and with the privacy policies, procedures and practices of the hospital. 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.

[39] The hospital has also included the step of having users click "Agree" before they are able to access the system, and thereby the personal health information of hospital patients.

Privacy Training & Awareness Programs

[40] The hospital's privacy office indicates that it has been active in promoting good privacy practices and communicates regularly with hospital agents regarding appropriate access to personal health information and other privacy-related issues.

[41] In response to this breach, the hospital sent out an email to all staff reminding them of the importance of patient privacy and that snooping into patient records is a breach of *PHIPA* and that the consequences for privacy breaches are severe.

[42] As part of the hospital's orientation of new agents, privacy training is provided. The hospital also requires its agents to complete an online annual privacy training

course.

[43] This privacy training program covers a wide range of privacy-related topics, including: the purposes for which agents are permitted to collect, use and disclose personal health information; any limitations, conditions or restrictions imposed by the hospital on the collection, use and disclosure of personal health information; the obligations imposed on agents under *PHIPA* and its regulations; notice that the hospital conducts audits of collections, uses, and disclosures of personal health information; and the potential consequences for the custodian arising from agents who collect, use or disclose personal health information in contravention of *PHIPA*.

[44] The hospital requires that all of its agents complete and pass a privacy quiz to ensure their comprehension of the hospital's requirements surrounding the protection of personal health information.

Technical Measures or Safeguards

[45] In the following, I focus on one aspect of the hospital's technical measures to protect the privacy and security of personal health information, its auditing functionality.

Audit Functionality

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

> [a]udits are an essential technical safeguard to protect personal health information. They can be used to deter and detect collections, uses and disclosures of personal health information that contravene [*PHIPA*]. In this way, they help to maintain the integrity and confidentiality of personal health information stored in electronic information systems.

[47] In this case, the hospital's electronic health records system has been in place since 1994. The hospital acknowledges that although its current system is outdated, it still does have the ability to perform audits, albeit with limited functionality. It is through this auditing system that the hospital was able to detect this breach.

[48] Although the hospital's current limited auditing capabilities did not hinder its ability to detect this particular breach, there may be other circumstances where it would have. For example, although an employee may have a legitimate reason for accessing a limited amount of patient personal health information in order to perform their duties, that same individual may not have a permissible reason for accessing other records of personal health information for the same patient. In order to detect this latter form of unauthorized access, it would be necessary for the hospital to be able to determine whether a particular type of personal health information was accessed – something that its current electronic health records system is unable to do.

[49] Recent amendments to *PHIPA*, although not yet in force, describe the information that the organization responsible for the provincial electronic health record is required to maintain in audit logs (section 55.3). While I recognize that these new requirements do not apply to the hospital, these legislative amendments provide a good summary of the elements that a strong auditing program should contain. Among other things, the amendments require audit logs maintained by these organizations to include a record of the type of information that is viewed by users of an electronic health record.

[50] The hospital agrees that this type of functionality is highly desirable in the investigation of suspected breaches, but does not believe that this would materially change its ability to detect and deter privacy breaches. It states that, even with the limitations of the existing system, its robust privacy practices resulted in this breach being detected early on and proactively. Nevertheless, it also states that it is engaged in working with other hospitals in its region to explore the option of a regional electronic health records system to replace its current electronic health records system, and that it will include language in the request for vendor proposals that appropriately weights the importance of this system functionality.

[51] I am satisfied that, in this case, the absence in this hospital's audit logs of the "type" of information viewed did not hinder the hospital's ability to detect this particular breach. It did not hinder its investigation nor, it appears, the eventual prosecution of the employee involved.

[52] For the reasons I have expressed above, however, it is desirable that any future auditing system at the hospital has the ability to record not only that an employee accessed the personal health information of a patient, but which type of personal health information was viewed. I am encouraged that the hospital is taking steps to include this capability in the procurement process for a new electronic health records system. The opportunity is available for the hospital to ensure that the new system contains this capability, and I strongly recommend that it do so.

[53] Having regard to the above-described policies and practices, and in the circumstances of this particular breach and the hospital's response to and investigation of the breach, I am satisfied that the hospital complied with section 12(1) of *PHIPA*. No review will be conducted under Part VI of *PHIPA*.

DECISION:

[54] For the foregoing reasons, no review will be conducted pursuant to Part VI of *PHIPA*.

Original Signed by: December 18, 2017

Trish Coyle

Investigator