Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 69

HR16-87

A Public Hospital

February 13, 2018

Summary: A public hospital (the hospital) contacted the Office of the Information and Privacy Commissioner of Ontario (IPC) to report a privacy breach under the *Personal Health Information Protection Act, 2004* (*PHIPA*). This breach involved an allegation that a former hospital employee accessed and removed personal health information from the hospital's premises without authorization, in contravention of *PHIPA*. The hospital reported this matter to both the police and to the former employee's regulatory college. In light of the steps taken by the hospital to address this breach, 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), 12(2), 29, and 37(1).

INTRODUCTION:

[1] A public hospital (the hospital) contacted the IPC to report a privacy breach under the *Personal Health Information Protection Act, 2004* (*PHIPA*). This breach involved a hospital employee (the employee) removing 15 health records, 36 research files, and 2 data collection sheets, from the hospital's premises, without authorization. The hospital also reported that an audit of its electronic health records system had confirmed that the employee had inappropriately accessed the personal health information of 10 individuals and that it was possible that she had also inappropriately accessed the personal health information of four others.

BACKGROUND:

[2] On May 18, 2016, the hospital discharged the employee – a registered health professional who had been employed by the hospital as a Research Coordinator – for performance deficiencies.

[3] Following the employee's discharge, an individual informed the employee's supervisor that during the employee's tenure at the hospital, they had seen – on two separate occasions – paper health records in the back of the employee's vehicle. Upon learning this information, the supervisor contacted the Health Data Resources Department to determine which client health records were currently signed out under the employee's name.

[4] On May 30, 2016, in response to the supervisor's inquiry, the Health Data Resources Department contacted the hospital's Privacy Officer to inform her that the paper health records for 14 clients were signed out by the employee as part of her work on a research study that had been approved by the hospital's Research Ethics Board (REB). The REB conducts initial and ongoing reviews and monitoring of ethical issues of research involving human participants to ensure ethical acceptability. At this time, the hospital launched a formal internal investigation to determine whether there had been a privacy breach.

[5] As part of its investigation, the hospital's Manager of Health Information Management conducted a search of the employee's workstation. Through this search, two of the 14 paper client health records were found in a desk drawer, leaving 12 paper client health records that had been signed out by the employee, unaccounted for.

[6] In a further attempt to locate the missing health records, the hospital conducted a search of its Health Data Resources Department. Unfortunately, none of the 12 missing paper client health records were found during this search.

[7] Another step in the hospital's investigation included an audit of its electronic health records system. One important requirement of REB-approved research studies is that researchers require the consent of study participants to access their electronic health records through the hospital's electronic health records system.

[8] Through the hospital's audit, it learned that despite the employee not having the consent of 10 study participants to review their electronic health records, she did so anyway. The audit also showed that the employee may have also inappropriately accessed the electronic health records of four additional research participants.

[9] Upon completion of its internal investigation, the hospital confirmed that the types of personal health information contained in the 12 missing paper health records included research subjects' names and health card numbers, as well as diagnostic information, treatment assessments and progress notes.

[10] The hospital confirmed that its auditing system records the types of electronic health records that an employee has accessed. These types of records, among other things, include a medical summary, hospital appointments, medical care activity, medical imaging scans, and results of other medical reports.

[11] The hospital also confirmed that the types of personal health information contained in the 14 electronic health records that had been, or may have been, inappropriately accessed, included research participants' names, addresses, health card numbers, diagnoses, brain imaging results, detailed information about the research subject's medical history and the type of care provided to them. This information also included details about research subjects' biological mothers.

[12] Altogether, with the missing files and inappropriate access/possible inappropriate access to electronic health records, 79 individuals were affected by this breach. In some cases, files contained the personal health information of more than one individual – of the 79 affected parties, 47 were research participants/clients, and 32 were biological mothers.

[13] The hospital's investigation concluded that by removing the paper health records of study participants from the hospital's premises and by inappropriately accessing the electronic health records of study participants without their consent, the former employee acted contrary to both hospital policy and the REB's consent requirements.

[14] Upon completion of its investigation, the hospital notified the police about the missing paper health records. The police interviewed the former employee, asking her to return any hospital files that she still had in her possession. In response, the employee provided the police with hospital manuals, blank data collection sheets, and a variety of other documents. None of the items returned by the employee contained any personal health information and the employee informed the police that she did not have additional documents or records in her possession.

[15] Although the hospital states that the employee's actions were inappropriate and unauthorized, the hospital has stated that it does not believe that the employee was acting with any malicious intent.

DISCUSSION:

[16] There is no dispute that the person who operates the hospital is a "health information custodian" and that the records at issue are records of "personal health information", which included research study participants' names, addresses, health card numbers, diagnoses, brain imaging results, detailed information about the research subject's medical history and the type of care provided to them. The missing information also included information about research subjects' biological mothers, including pregnancy and delivery information. Altogether, 79 individuals were affected

by this privacy breach – of these, 47 were research participants/clients, and 32 were biological mothers.

[17] Based on the information set out above, as a preliminary matter, I find that the person who operates the hospital is a "health information custodian" under paragraph 4.i of section 3(1) of *PHIPA*, and that the records at issue contain "personal health information" under sections 4(1)(a), (b), and (f) of *PHIPA*, which were in the custody or control of the hospital.

[18] I further find that the employee was an "agent" of the hospital, as that term is defined in section 2 of *PHIPA*.[1] The hospital does not dispute this finding.

ISSUES:

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

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

2. Is a review warranted under Part VI of *PHIPA*?

RESULTS OF THE INVESTIGATION:

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

[20] 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;[2]
>
> "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;

---

[1] *PHIPA* Orders HO-002, HO-010, and HO-013.

[2] This definition of "use" was in force at the time of these events. The definition has since been amended.

[21] Under *PHIPA*, personal health information is permitted to be used or disclosed if the use or disclosure complies with section 29, which states:

> Requirement for consent
>
> 29. A health information custodian shall not collect, use or disclose personal health information about an individual unless,
>
> > (1) 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
> >
> > (2) the collection, use or disclosure, as the case may be, is permitted or required by this *Act*.

[22] The hospital made multiple attempts to contact the former employee, both verbally and in writing, to ask her if she had any health or research files in her possession. The employee did not respond to any of the hospital's attempts to contact her.

[23] When the former employee was interviewed by the police about this matter, she brought with her general hospital documents to be returned to the hospital. These documents consisted of training materials and blank data collection forms. They did not include any personal health information or missing files.

[24] As part of the IPC's investigation into this breach, this Office also contacted the former employee to ask her about the missing files. The employee informed the IPC that, prior to her termination, she had been working with two paper health records and that these records would still be in a cabinet at her workstation on hospital premises. According to the employee, although these records were never removed from hospital premises, they had not been signed out from the Health Data Resources Department. The employee further stated that she had no knowledge of the 12 missing files and disputed ever taking any health records home.

[25] The employee explained that it was not the hospital's practice to require staff to receive a response to their email requests to remove paper health records from the Health Data Resources Department, as long as these records were being reviewed on hospital premises. With respect to the missing health records, the employee stated that she had sent an email to the Health Data Resources Department to request the now missing health records but that she had not received a response.

[26] Further, the employee stated that, unlike health records, research files were routinely removed from the hospital by research staff to attend off-site visits at research subjects' homes and to review data. The employee stated that the hospital was aware of this practice and that, in support of her position, the hospital reimbursed her for her mileage to and from these off-site visits to research participants' homes.

[27] Although the hospital disagrees, the employee maintains that she had been told by staff in the Health Data Resources Department that signing health records out was not a requirement – that the process was to send an email request to Health Data Resources Department for the records and to provide them with a copy of study participants' consent forms to have research staff view their personal health information.

Use of Personal Health Information

[28] Both the inappropriate access and loss of health records are serious matters, as they can affect the health care a patient receives as well as their confidence in the healthcare system as a whole.

[29] In keeping with the plain meaning of the phrase "to handle or deal with the information," as set out in section 2 of *PHIPA*, I find that both accessing the personal health information of research subjects via the hospital's electronic health records system without their consent and losing paper health records would both be considered "uses" within the meaning of section 2 of *PHIPA*.

[30] There is no information or evidence before me to suggest that the research subjects in question consented to their personal health information being accessed by the employee or that the employee could assume the patients' implied consent.[3]

[31] With respect to the health records that cannot be located, there is no evidence before me to suggest that the records were intentionally stolen. The hospital and the former employee disagree on exactly what happened to the missing records. Specifically, the former employee disputes taking any health records home.

[32] For the purposes of this Decision, while I am unable to resolve the dispute as to exactly how the records were lost, it is not necessary for me to do so – either they were lost because the employee took them home and did not return them, or they were lost by the hospital in some other way. Regardless, as a result of this loss, the requirement in section 12(2) of *PHIPA* to notify affected individuals that their personal health information has been breached, is triggered. Pursuant to this requirement, the hospital did notify all affected individuals of the breach.

[33] 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 any of the employee's uses of personal health information (via accessing or possibly accessing research subjects' personal health information) were for a purpose set out in section 37. In fact, the hospital has stated that the personal health information was used without the research participants' consent and that these uses were not permitted by section 37 of *PHIPA*.

---

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

[34] The hospital has taken the position that the "use(s)" of personal health information did not comply with *PHIPA* and there is no evidence before me to suggest that this use was for a purpose consistent with section 37 of *PHIPA*.

[35] The hospital agrees, and I find, that the personal health information was used in manners that were not consistent with section 37 *PHIPA*. Accordingly, I find that the uses of personal health information at issue did not comply with *PHIPA*.

Disclosure of Personal Health Information

[36] During the employee's conversations with the police, she stated that she had not disclosed any personal health information. The hospital has also stated that it has no reason to believe that any personal health information was disclosed.

[37] Based on the information set out above, there is no evidence before me to suggest that the employee, herself, disclosed records of personal health information.

Issue 2: Is a review warranted under Part VI of *PHIPA*?

[38] Section 12(1) of *PHIPA* requires that health information custodians take "reasonable" steps to protect personal health information against theft, loss and unauthorized use and 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 unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

[39] In this case, there is no disputing records of personal health information were lost. The hospital acknowledges that study participants' personal health information was accessed electronically, without their consent. This amounted to a use that was not consistent with *PHIPA*.

[40] In *PHIPA* Order HO-013, Commissioner Brian Beamish summarized this office's approach to "reasonable steps" in section 12(1) of *PHIPA:*

> 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. …

[41] In the IPC's publication, "What to do When Faced With a Privacy Breach: Guidelines for the Health Sector,"[4] this office set out recommendations for health information custodians when responding to a privacy breach. The four steps described in this publication are:

Step 1: Respond Immediately by Implementing the Privacy Breach Protocol

[42] As soon as it learned of the breach, the hospital implemented its Privacy Breach Protocol, which requires starting an internal investigation, notifying appropriate hospital staff and, in serious cases, notifying the IPC and other authorities.

[43] In this case, the hospital reported the breach to the police. The police investigated this matter and interviewed the former employee. The employee provided the police with administrative hospital documents that she still had in her possession – these included training manuals and blank data collection forms. The employee provided the police with a statement that she did not have any additional documents or records in her possession. No criminal charges were laid.

Amendments to PHIPA

[44] In May 2016, the Ontario government passed new health privacy legislation which, among other things, makes it mandatory to report privacy breaches to the Information and Privacy Commissioner and regulatory colleges, in specific circumstances.

[45] Although these amendments to *PHIPA* were not in force at the time of the breach nor when the hospital first learned of this breach, it proactively and voluntarily reported this breach to the IPC.

---

[4] https://www.ipc.on.ca/wp-content/uploads/Resources/hprivbreach-e.pdf

[46] In addition, in consultation with the IPC throughout the course of this investigation, the hospital agreed to report this matter to the former employee's regulatory college.

Step 2: Containment – Identify the scope of the potential breach and take steps to contain it

[47] As part of the hospital's efforts to contain the privacy breach, it made several attempts to contact the former employee to obtain information about the missing records and, if possible, to arrange to have these records returned.

[48] In addition to numerous telephone calls, the hospital also sent three formal letters to its former employee. One letter stated, in part:

> Health Data Resources has recently identified that numerous client health records have been removed from their office and have not yet been returned. According to our records, these documents were last signed out under your name and we are hoping that you may be able to help us locate them. If the files are with you, we would be pleased to send a courier to retrieve them at a time that is convenient for you. Alternatively, if you have any information as to where the files might be we would be grateful for your advice in this regard.

[49] In another letter to the former employee, the hospital stated, in part:

> We require your assistance in determining the location of these missing client/research files. As a former employee of (the hospital) and a member of (a regulatory college) you are obligated by law to provide that assistance.
>
> We must emphasize the seriousness of this matter and the need for your full cooperation. We have been in contact with the Information and Privacy Commissioner of Ontario and will be in contact with (the police) and (your regulatory college) if we do not hear from you by Thursday June 16 at 9:00 a.m.

[50] As discussed earlier in this Decision, the IPC also had communication with the former employee and inquired about the missing health records. According to the employee, she had never removed health records from hospital premises. She did, however, admit to taking research files off-site.

Step 3: Notification – Identify those individuals whose privacy was breached and notify them of the breach

[51] The hospital notified affected individuals by way of a phone call, which was followed up by sending out a detailed letter, outlining the circumstances surrounding

the breach, the steps the hospital has taken to enhance its privacy policies in response to the breach, as well as contact information for the IPC in the event any affected individuals wished to make a complaint to this office.

[52] At the time of the breach, although section 12(2) did not include the requirement to also notify affected individuals that they may make a complaint to the IPC regarding the breach, the hospital's notice included this information.

Step 4: Investigation and Remediation

[53] Below, I will discuss the administrative measures and safeguards that the hospital has in place for protecting both paper and electronic records, relevant to this breach. As part of its investigation into this breach, the hospital confirmed with the IPC that, through its electronic health records system, it is able to audit employees' access to various types of medical records on its electronic health records system. These types of records, among other things, include a medical summary, hospital appointments, medical care activity, medical imaging scans, and results of other medical reports.

[54] It was through the hospital's auditing abilities that it was able to confirm that the employee had inappropriately accessed research participants' personal health information.

Privacy Policies & Procedures

[55] As previously mentioned, at the time of the breach, the hospital's REB required that, in order to access the personal health information of research participants, researchers required the consent of study participants. When this breach occurred, the hospital did not have a specific policy in place to ensure that researchers had the consent of study participants prior to accessing their personal health information.

[56] Although the hospital's policies were silent on whether researchers required the consent of research participants to access their personal health information, given that obtaining this consent was a requirement of the hospital's REB, at the time of the breach, the employee was required to have participants' consent in order to access their personal health information.

[57] As a result of the breach, the hospital has revised its privacy-related policies to ensure greater control over all health records. At the time of the breach, although the hospital's policy was clear that health records could not be removed from the hospital, it was silent on research files.

[58] Since the breach, the hospital has made changes to ensure that its research files are anonymized. These changes have also included the fact that the hospital now has a formal process in place requiring that personal health information is stored in a separate physical location from the research file.

[59] As part of the hospital's investigation into this breach, it learned that there had been ambiguity among research staff and supervisors about removing research files from hospital premises – specifically, that the removal of research files containing personal health information was discouraged, but not prohibited. This is consistent with the former employee's statement regarding the removal of research files from the hospital.

[60] Another step that the hospital has taken is that it has enacted a strict sign-out process for paper health files and has limited the number of these records that researchers are able to sign out at one time. The hospital has also reduced the timeframe for which health records can be removed from the Health Data Resources Department by authorized staff.

[61] Further, the hospital has amended its Human Resources Checklist for employees leaving the organization so that any health records that an employee has signed out are returned to the organization prior to the employee's departure. It has also implemented a process to track which health records and research files are in an employee's possession.

Confidentiality Agreements

[62] Prior to the breach, research staff at the hospital were not required to sign a confidentiality agreement. Since the breach, however, this has changed. The hospital now requires all employees to sign a confidentiality agreement at the time of hire and annually, as part of their annual performance review.

[63] Because the former employee was initially hired by the hospital in a clinic role, she did sign a Confidentiality Agreement at the time of her hire in 2011.

Privacy Training

[64] The hospital's privacy training and awareness system includes in-person privacy training on Day 1 of an employee's orientation. New hires are also required to complete and pass an online privacy training module.

[65] In response to this breach, the onboarding process for new staff at the hospital now includes interactive privacy training on the Regulatory Framework for health privacy, real-life examples of privacy breaches (including the one that is the subject of this investigation), and details about sanctions associated with privacy breaches.

[66] The hospital's training also specifically addresses that staff are prohibited from removing any files containing personal health information from the hospital – including taking work home to complete projects or catch up on tasks. In addition, the hospital also requires its staff receive annual privacy training and that they complete and pass an online privacy test.

[67] Following this breach, in addition to its regular privacy training that all staff receive, the hospital decided to provide additional mandatory privacy training for all research employees, students, trainees, and volunteers who are involved in clinical trials. Before starting a clinical trial, individuals in the above-noted positions are also now required to complete two modules through the "Collaborative Institutional Training Initiative Program" – "Good Clinical Research Practice" and "Responsible Research Conduct." Refresher courses on these two modules is required to be completed every three years. These additional training requirements have been communicated to current staff.

[68] The hospital's privacy policies and practices reviewed above are consistent with the IPC's guidance, such as *Detecting and Deterring Unauthorized Access to Personal Health Information*.[5]

[69] Having regard to the above-described policies and practices and the hospital's response and investigation into this breach, I am satisfied that the has hospital responded adequately. No review will be conducted under Part VI of *PHIPA*.

DECISION:

[70] For the foregoing reasons, no review of this matter will be conducted under Part VI of *PHIPA*.

Original Signed by: February 13, 2018
Trish Coyle
Investigator

[5] *Supra* note 4 at page 13.