Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 151

Complaint HI18-6

[A medical clinic]

July 15, 2021

Summary:

The office of the Information and Privacy Commissioner of Ontario received a complaint under the *Personal Health Information Protection Act, 2004* (the *Act*) against a medical clinic (the Clinic). The complaint involved a second incident in which a physician working at the Clinic left a patient alone in a waiting room that had a computer screen displaying the physician's schedule, which contained personal health information of 35 patients.

This decision finds that the Clinic failed to take reasonable steps to ensure the protection of the personal health information against unauthorized disclosure as required by section 12(1) of the *Act*. I also find that the Clinic did not notify the affected patients as is required by section 12(2) of the *Act*. However, in light of the steps taken by the Clinic to address the privacy breach, which included notifying the affected patients, I am satisfied with the Clinic's response to the breach and it is unnecessary for this matter to proceed to adjudication to consider potential orders.

Statutes Considered: *Personal Health Information Protection Act, 2004,* sections 2, 3(1), 4(1) and (2), 12(1) and (2), 29, 58 and 60(13).

Decisions Considered: PHIPA Decisions 110 and HO-013

BACKGROUND:

The first incident:

[1] On August 9, 2017, under the *Personal Health Information Protection Act, 2004*

(the *Act* or *PHIPA*), the Office of the Information and Privacy Commissioner of Ontario (the IPC or this office) received a complaint from a patient regarding a medical clinic (the Clinic). According to the patient, she was left alone in an internal waiting room with an unlocked computer screen that displayed the physician's schedule and other patients' information, including details about their medical conditions.

[2] File HC17-60 was opened at the Intake Stage of the IPC's complaint process and an IPC Analyst worked with the Clinic to address the issues raised by the complaint. At that time, the Clinic committed to implementing several remedial measures to avoid the reoccurrence of a similar incident.

[3] On December 4, 2017, in response to the complaint, the Clinic advised this office that it had conducted refresher privacy training for all of its staff and physicians on its existing privacy policies. This training included information about computer security and the specific direction that any computers left unattended must be locked. The Clinic confirmed that it posted signage in every room to remind its staff and physicians of their privacy obligations and changed the position of its computer monitors so that they no longer faced patients or other individuals not employed by the Clinic. Based on the Clinic's confirmation that it had implemented these measures, as well as the complainant's confirmation that her concerns had been addressed, file HC17-60 was closed on December 11, 2017.

The second incident:

[4] On February 14, 2018, the IPC received a second privacy complaint about the Clinic from a patient, who again was left alone in an internal waiting room with other patients' information visible on a computer screen.

[5] According to the patient, on January 31, 2018, she was left alone in an examination room with an unlocked computer screen and as a result, was able to see the physician's schedule for the day, along with the health information of other patients, including their names, symptoms and purpose of their visit.

[6] The patient explained that, at one point, the receptionist came into the examination room and minimized all of the program windows on the computer screen, except for one patient's lab results. However, the screen remained unlocked and the patient was left in that room for about 10 minutes.

[7] After becoming aware of this second incident, the IPC had concerns about the Clinic's information and security practices for protecting personal health information. As a result, a Commissioner-initiated complaint file was opened at the Intake stage of the IPC's *PHIPA* process and was assigned to an Analyst. The Analyst made inquiries with the Clinic but was not satisfied with the responses provided and continued to have ongoing concerns with the lack of information provided by the Clinic.

[8] As such, the matter moved to the Investigation Stage of the IPC's *PHIPA* process and I was assigned as the Investigator. As part of my investigation, I requested and

received written representations, discussed below, from the Clinic. In addition, because the Clinic was raising concerns about whether the photograph was authentic, this office issued a Notice of Review under section 58 of the *Act* and a determination under section 60(13) of the *Act,* so that the photograph could be shared with the Clinic.

Preliminary matters:

[9] There is no dispute, and I find, that the person who operates the Clinic is a "health information custodian" within the meaning of section 3(1) of the *Act*.

[10] Further, the Clinic does not dispute, and I find, that the physician is its agent within the meaning of section 2 of the *Act*. This section defines an "agent" as follows:

> "agent", in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated;

[11] With respect to the personal health information at issue, in order to report this matter to the IPC, the complainant took a photograph of the unlocked screen and provided this office with a copy of it. My review of the photograph found that the screen shows the physician's schedule, which contained names of 35 patients of the Clinic. More specifically, it shows the symptoms experienced by these patients and the purpose of their visit to the Clinic (for example depression, swollen face, etc.). After providing the photograph to this office with her complaint, the patient confirmed that she deleted the photograph and did not retain a copy.

[12] The Clinic does not dispute, and I find, that the information at issue that was displayed on the unlocked screen is personal health information within the meaning of section 4(1) of the *Act*. "Personal health information" is defined in this section, in part, as follows:

> "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,

[13] Moreover, section 4(2) of the *Act* defines "identifying information" as follows:

> "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.

[14] Regarding the disclosure of the personal health information, section 29 of the *Act* states:

> 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] The Clinic does not dispute, and I find, that the disclosure of the personal health information at issue was not permitted on the basis of consent or another authority under the *Act*, and, therefore, was a privacy breach under the *Act*.

ISSUES:

[16] This decision addresses the following issues:

1. Did the Clinic take reasonable steps in the circumstances to ensure the protection of the personal health information against unauthorized disclosure in accordance with section 12(1) of the *Act*?

2. Did the Clinic notify the individuals affected by the unauthorized disclosure of the personal health information in accordance with section 12(2) of the *Act*?

3. Have the issues been resolved to the IPC's satisfaction, or should this matter proceed to the Adjudication Stage of the IPC's *PHIPA* process to consider potential orders?

DISCUSSION:

Issue 1: Did the Clinic take reasonable steps in the circumstances to ensure the protection of the personal health information against unauthorized disclosure in accordance with section 12(1) of the *Act*?

[17] As previously indicated, this matter concerns the reoccurrence of an unauthorized disclosure of personal health information by the Clinic due to an unlocked computer screen. Accordingly, it raised concerns about whether the Clinic had adequate security measures in place to protect this information in accordance with the *Act*.

[18] Section 12(1) of the *Act* requires that custodians take "reasonable" steps to protect personal health information against unauthorized disclosure. This section 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.

Administrative and Technical Measures and Safeguards:

[19] Administrative and technical measures and safeguards are critical to protecting personal health information. 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.

[20] The IPC has also stated that, in order to comply with the requirement in section 12(1) of the *Act,* custodians must implement administrative and technical measures or safeguards, including privacy policies, procedures and practices, as well as privacy training, awareness programs and initiatives.[1] The duty to take reasonable steps to protect personal health information includes a duty to respond adequately to a complaint of a privacy breach. Among other things, a proper response to a breach will help ensure that it is contained and will not re-occur.

[21] According to the Clinic, it has a standard waiting area located 20 feet away from the reception area, six treatment rooms and one lab. All of the treatment rooms contain a computer with only the assigned physician and the receptionist having access to these rooms.

[22] In order to access the electronic patient management/scheduling system in a computer, the physicians must enter a password that they are required to create, manage and keep private. The Clinic explained that all of the computers have a 60-second default setting, which locks the computer when it is not in use, and that all of its staff and physicians are trained to manually lock them in order to prevent any unauthorized access.

[23] In the circumstances of this complaint, the Clinic advised that the physician was responsible for manually locking the computer because it was not in use.

[24] The Clinic also confirmed that, at the time of the breach, the Clinic's electronic

---

[1] PHIPA Decision 110

patient management/scheduling system did not display a privacy warning or require its staff and physicians to agree to any terms of use when logging on.

The Clinic's Privacy Policy:

[25] At the time of the breach, the Clinic had a privacy policy (the policy) that it kept in a binder at the front desk of the reception area. The policy is available to all of the Clinic's staff and physicians and states:

> [The Clinic]…values patient privacy and acts to ensure that it is protected. This policy has been written to capture [the Clinic's] current practices and to respond to federal and provincial requirements for the protection of personal information. This policy describes how [the Clinic] collects, protects and discloses the personal information of patients and the rights of patients with respect to their personal information.

[26] Section 2 of the policy states that "The [Clinic] has appointed a Security Officer who has the overall responsibility to manage the privacy and security program on a day-to-day basis, in accordance with the Lead Physician" and that the Clinic "employs strict privacy protections." This section also explains that the Clinic educates and trains staff on the importance of protecting personal information on an ongoing basis.

[27] Further, section 4 of the policy requires that staff[2] "sign a Security Acknowledgement and Confidentiality Agreement as part of their employment contract."

[28] The policy also includes a section titled *Privacy Breach Protocol* that describes the steps that must be taken when a privacy breach occurs and also includes information regarding the responsibilities of staff to protect and secure patients' personal health information.

[29] Moreover, under the heading "Guidelines on what Health Information Custodians should do in the event of breach" section, there is a list of detailed steps that must be immediately taken by the Clinic's staff and physicians in response to a privacy breach. These steps are as follows:

> Step 1: Respond immediately by implementing the privacy breach protocol
>
> Step 2: Containment - Identify the scope of the potential breach, take steps to contain it
>
> Step 3: Notification - Identify those individuals whose privacy was breached and notify them of the breach

---

[2] The Clinic confirmed that the policy's reference to "staff" includes its physicians. Based on this office's recommendation, the Clinic confirmed that it will amend the policy to make this inclusion clearer.

Step 4: Investigation and Remediation

[30] Under the heading "How to Protect Information" in the policy, the Clinic's staff and physicians are required to:

- Understand security as it relates to your role and your obligations;
- Always lock your screen when you are away from your computer and log out of PS; and
- Install a privacy screen over your monitor to make it difficult for casual visitors in your office to read the contents displayed.

[31] The policy also requires that its staff and physicians:

- Read, sign and comply with the Privacy Policy;
- Read and follow the best practices for security in the Security Best Practices Guide; and
- Avoid accidentally exposing sensitive information through conversations, exposed computer screens and unattended desks.

[32] In addition, the policy's "Appendix 3: Roles and Responsibilities for Security" lists the duties of the Clinic's security officer and includes the following:

- Ensuring the Privacy Policy is available to both staff and patients.
- Ensuring staff and contractors are aware of the Privacy Policy and informed on how it should be interpreted and put into action.
- Ensuring all staffs are trained on their security responsibilities.
- Collecting and filing the signed and dated Security Acknowledgement and Confidentiality Agreement from all staff and necessary third parties.

Training

[33] At the time of the breach, the Clinic advised that it was only providing privacy training to its staff upon hire. However, since the breach, the Clinic advised it has provided refresher privacy training to all of its staff and physicians and has committed to annual mandatory privacy training.

[34] Further, the Clinic advised that it created a privacy policy booklet and questionnaire that its staff are now required to review and complete on an annual basis. The Clinic also advised that completed questionnaires by staff are kept in their employment folder.

[35] The Clinic also confirmed that the policy is reviewed at quarterly meetings at

which staff also discuss any privacy concerns that they may have.

[36] Since the second privacy breach, the Clinic advised that it has been conducting mandatory privacy meetings once a month with all of its staff. The Clinic explained that in these meetings, staff discuss methods of keeping the personal health information of the Clinic's patients private and that staff are reminded of the following:

1. no papers should be left on desk;
2. to make sure all scrap paper goes to the shredder;
3. when leaving a desk, they should make sure the computer is locked; and
4. they should never give out passwords.

[37] According to the Clinic, there are signs posted by computers in every examination room reminding staff and physicians of their privacy obligations and staff have been provided with a copy of the IPC's publication "Detecting and Deterring Unauthorized Access to Personal Health Information".

Confidentiality Agreements:

[38] Contrary to section 4 of the Clinic's policy, at the time of the breach, the Clinic did not require its staff to sign confidentiality agreements.

[39] Regarding these agreements, the IPC's "Detecting and Deterring Unauthorized Access to Personal Health Information" guidance document states:

> Requiring agents to sign confidentiality agreements on a regular basis may also help to prevent or reduce the risk of unauthorized access to personal health information. Confidentiality agreements require agents to acknowledge the privacy obligations and expectations, including the consequences of a privacy breach.

[40] Going forward, the Clinic advised that all of its staff and physicians will now sign confidentiality agreements on an annual basis. The Clinic also confirmed that it will keep copies of signed agreements in its employee personnel files.

Technical Safeguards:

[41] Section 4 of the policy also contains a list of administrative and technological safeguards that are in place to prevent an unauthorized disclosure of personal health information, such as:

- Protected computer access for patient health information
- Passwords
- User authentication

- System protections
- Firewall software

[42] Further, section 5 of the policy, "Password Guidelines", directs the Clinic's staff and physicians to do the following:

- Ensure that your computer has a screen saver that activates after a predefined time and requires a password to gain access to the computer.
- It is recommended that you change your passwords frequently, at least every 90 days.
- Passwords must NEVER be disclosed to anyone or written down.
- A password should:
    - Contain a minimum of eight characters
    - Include a combination of upper and lower case letters, numbers and/or special characters
    - Should not be obvious, easily guessable, or found in a common words dictionary
    - Should not use acronyms, birthdays, sequential numbers, names of family members or pets
- If you suspect the confidentiality of your password has been compromised, change it immediately

[43] As previously indicated, all of the Clinic's computers have a 60-second default lock. Since the second incident, the Clinic has provided training to its staff and reminded them that they are responsible for manually locking their computers when they are not in use or when stepping away from a computer. Once locked, the Clinic advised that a password is required in order to gain entry back into the computer.

[44] In response to inquiries made during my investigation, the Clinic advised that it implemented a privacy warning screen on its Electronic Management Record system. A copy of this warning screen was provided to the IPC and it states:

> Protect Patient Privacy - Personal Health Information Protection Act
>
> (PHIPA)
>
> I will not access personal health information unless I am providing care to the patient or unless access is required to carry out my assigned duties. I will protect patient's confidentiality and will only collect/use/disclose it for

> authorized purposes. I am accountable for my actions and understand the contravention of these privacy obligations may result in disciplinary actions, notification to College, a $100,000 fine and a civil action. I have read, understand and agree to comply with the clinics privacy, confidentiality, and security policies and Ontario's privacy legislation.

[45] The Clinic also advised that it installed a black-out privacy screen on all of its computers. The Clinic explained that the screen blacks out the computer screen when viewed from the side, but allows information on the screen to be visible from a straight-on view. Further, as indicated above, the Clinic confirmed that the computer monitors are set up to face away from the patients.

[46] In order to prevent a similar breach from reoccurring, the Clinic has also committed to sending an email every 3 months to its staff to remind them of their obligations under the *Act* and to lock the computers before leaving the examination room.

[47] With respect to the importance of privacy training, in Order HO-013, former Commissioner Brian Beamish stated:

> 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.[3]

[48] I agree and adopt this statement.

[49] At the beginning of this investigation, I was concerned with the adequacy of the Clinic's privacy policies, practices and training. An examination of events leading up to the second privacy breach also demonstrated that the Clinic did not adhere to all of the requirements of its own policy.

[50] First, the Clinic's staff and physicians failed to manually lock the computer when the complainant was left alone in the waiting room as required by the policy.

[51] Second, contrary to the policy, the Clinic did not require that its staff and physicians sign confidentiality agreements and did not have mandatory privacy training in place.

[52] Third, the Clinic did not follow its Privacy Breach Protocol. Initially, the Clinic made no effort to investigate the privacy breach allegation, determine the scope of the breach, or notify the individuals affected by the breach.

---

[3] HO-013, p. 36

[53] Accordingly, based on the aforementioned reasons, in the circumstances of this breach, I find that the Clinic failed to take reasonable steps to ensure the protection of the personal health information against unauthorized disclosure as required by section 12(1) of the *Act*.

[54] However, having regard to the Clinic's response to this breach, I am satisfied that the Clinic has resolved these issues and has now taken reasonable steps in the circumstances to ensure that the personal health information is protected against a similar unauthorized disclosure.

Issue 2: Did the Clinic notify the individuals affected by the unauthorized disclosure of the personal health information in accordance with section 12(2) of the *Act*?

[55] Section 12(2) of the *Act* requires that the Clinic notify the individuals whose personal health information was disclosed without authorization of the disclosure. This section states:

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

[56] It is important to note that, at the beginning of this investigation, the Clinic did not notify the individuals affected by the breach as required by section 12(2) of the *Act.* According to the Clinic, this notification was not provided to patients because the Clinic was uncertain of their identities and wanted to see the photograph to confirm it was authentic.[4]

[57] Further, the Clinic initially took the position that the photograph did not contain its patients' personal health information. As a result, the Clinic did not make an effort to determine the identities of the patients affected by the breach and did not want to notify all of the patients that attended the Clinic on the day of the second incident.

[58] It was only after the Clinic reviewed the photograph taken by the complainant

---

[4] As previously indicated, this office issued a Determination under section 60(13) of the *Act*, in order to provide the Clinic with a copy of the photograph.

that it acknowledged, as indicated above, that the photograph contained personal health information and took steps to notify the affected patients.

[59] To that end, the Clinic advised that a total of 88 patients attended the Clinic on January 31, 2018 and, based on a recommendation made by this office[5], sent notification letters to each of them on January 11, 2021.

[60] The notification letters included details about the circumstances of the breach, the steps that the Clinic took to enhance its privacy policies and the additional privacy training that was conducted in response to the breach. The letters also contained the contact information for the IPC, in the event that any of the affected individuals wished to make a complaint to this office. Further, the letters advised them that the photograph had been deleted and that no copies of it were retained.

[61] Based on the aforementioned, I find that, contrary to the policy, the Clinic did not notify the individuals affected by the unauthorized disclosure at the "first reasonable opportunity". Therefore, I find that the Clinic did not provide them with the notification required by section 12(2).

[62] However, in response to inquiries made during this investigation, I am satisfied that the Clinic has now taken steps to provide this notification.

Issue 3: Have the issues been resolved to the IPC's satisfaction, or should this matter proceed to the Adjudication Stage of the IPC's *PHIPA* process to consider potential orders?

[63] In the circumstances of this complaint, I found that the Clinic did not take the steps required by section 12(1) of the *Act* or provide the notification required by section 12(2) of the *Act*.

[64] However, as previously indicated, the Clinic has now taken a number of steps to address the privacy breach.

[65] In light of the steps taken by the Clinic, I am satisfied that the issues have been resolved, and it is not necessary for this matter to proceed to the Adjudication Stage of the IPC's *PHIPA* process to consider potential orders.

[66] Therefore, in accordance with my delegated authority under the *Act*, I have decided to conclude this review without referring this matter to the Adjudication Stage of the IPC's *PHIPA* processes and without an order being issued by the IPC.

Original Signed by: JULY 15, 2021

[5] This office recommended all patients who attended the Clinic on the day of the breach be notified as the Clinic was unable to confirm whose lab results were disclosed when the computer remained unlocked.

Soha Khan
Investigator