Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 184

Complaint HI19-00050

A Medical Clinic

July 5, 2022

Summary: The office of the Information and Privacy Commissioner of Ontario received a complaint under the *Personal Health Information Protection Act* (the *Act*) against a medical clinic. The complaint alleged that the clinic had inadequate privacy practices with respect to the security and safeguarding of the personal health information of its patients. The decision finds that the clinic did not have reasonable measures in place to ensure the protection of the personal health information of its patients as required by section 12(1) of the *Act*. However, in light of the steps taken by the clinic to address the issues identified, no review of this matter will be conducted under Part VI of the *Act*.

Statutes Considered: *Personal Health Information Protection Act, 2004, S.O. 2004,* section 12(1)

Decisions Considered: HO-010, HO-013, PHIPA Decisions 64 and 70

BACKGROUND:

[1] On December 18, 2019, pursuant to the *Personal Health Information Protection Act, 2004* (the *Act*), the Information and Privacy Commissioner of Ontario (the IPC or this office) received a complaint against a medical clinic (the clinic or custodian). The complaint alleged that the clinic had inadequate privacy practices with respect to the security and safeguarding of the personal health information of its patients.

[2] Specifically, the complaint identified the following concerns:

- clinic staff use their personal emails for work-related purposes;
- staff share passwords for user accounts on the system;
- passwords are taped to desks or walls in plain sight of visitors;
- the clinic does not complete system security patching and there is insufficient virus protection software; and
- some computers at the office use Windows 7, which is no longer supported by Microsoft and therefore vulnerable to cyberattacks.

[3] This investigation does not deal with a specific breach incident, but rather is an analysis of the clinic's practices and policies to protect and secure the personal health information of its patients.

PRELIMINARY ISSUE:

[4] There is no dispute that the clinic is a "health information custodian" within the meaning of section 3(1) of the *Act* and that the records generated through the clinic's services are records of personal health information pursuant to section 4 of the *Act*.

ISSUES:

[5] This decision addresses the following issues:

1. Did the clinic have reasonable steps in place to protect personal information?
2. Is a review warranted under Part VI of the *Act*?

RESULTS OF THE INVESTIGATION:

Issue 1: Did the clinic have reasonable steps in place to protect personal information?

[6] The *Act* requires health information custodians to take "reasonable" steps to protect personal health information in their custody and control against unauthorized use or disclosure, among other things.

[7] Specifically, section 12(1) of the *Act* 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.

[8] In this case, the allegations in this complaint raised questions about whether the custodian had reasonable measures in place to ensure the security and privacy of the personal health information of their patients.

[9] In Orders HO-010 and HO-013, and more recently in PHIPA Decisions 64 and 70, the IPC held that section 12(1) of the *Act* requires health information custodians to review their measures or safeguards from time to time to ensure that they continue to be reasonable in the circumstances to protect personal health information in the custodians' custody or control.

[10] Health information custodians are also expected to identify risks to privacy and take reasonable measures to reduce or eliminate such risks and mitigate the potential harms that may arise.[1]

[11] The IPC has previously stated that, in order to comply with the requirement in section 12(1) of the *Act,* custodians must take steps that are reasonable in the circumstances to protect personal health information and must implement administrative and technical measures or safeguards.[2] Such measures and safeguards can include privacy policies, procedures and practices, strong passwords, encryption, maintaining up to date software, firewalls, anti-virus, applying the latest security patches, as well as privacy training and awareness programs and initiatives.

[12] As part of my investigation, I examined the clinic's privacy practices and security measures, against the obligations in section 12(1) of the *Act.* As noted briefly above, there were a number of concerns raised about the clinic's privacy practices and security of personal information. Although I conclude that the clinic had inadequate privacy practices and administrative and technical safeguards in place, during my investigation into this matter, the clinic addressed the issues raised.

[13] I will explore the issues, concerns and the clinic's responses in more detail below.

Use of Personal Email Addresses:

[14] At the commencement of this investigation, the clinic confirmed that it was the clinic's practice to allow staff to use personal emails for clinic business with instructions not to include patient names. The clinic advised that staff were instructed to only use patient initials and/or medical record numbers or accession numbers when using personal emails.

---

[1] See HO-013
[2] Ibid

[15] The clinic also advised that it had been using a Gmail account to receive sensitive patient information such as requisitions as well as Picture Archiving and Communication System (PACS) confidentiality agreements from outside referrals.

[16] During this investigation the clinic provided this office with their policy titled "Personal Email use for work related purposes" which allows staff to use their personal email for work-related purposes and provides guidance for the use of personal email for work-related purposes. The policy includes details such as retention, disposal and the type of information that can and cannot be included in emails, that personal email accounts must be password protected and that personal accounts cannot be shared with any other individual.

[17] The IPC's guidance document entitled "Fact Sheet Communicating Personal Health Information by Email" sets out technical, physical and administrative safeguards. This document states the following:

> Custodians must implement technical, physical and administrative safeguards to protect personal health information. This requirement applies to any email communications involving this type of information. Technical safeguards include:
>
> - encryption for portable devices
> - strong passwords, and
> - firewalls and anti-malware scanners
>
> Physical safeguards include:
>
> - restricting office access, using alarm systems, and locking rooms where equipment used to send or receive health information by email is kept, and
> - keeping portable devices in a secure location, such as a locked drawer or cabinet, when they are unattended
>
> Administrative safeguards include:
>
> - providing a notice in an email that the information received is confidential
> - providing instructions to follow if an email is received in error
> - communicating by email from professional, rather than personal accounts (personal accounts may have weaker security levels and may be more susceptible to compromise)

- confirming an email address is up to date
- ensuring that the recipient's email address corresponds to the address proposed to be sent
- regularly checking preprogrammed email addresses to ensure that they are still correct
- restricting access to the email system and to email content on a need-to-know basis
- informing individuals of any email address changes
- acknowledging receipt of emails, and
- recommending that individuals implement the above safeguards, including that individuals communicate by email at an email address that is password protected, and is accessible only by them

Custodians should also ensure compliance with the safeguards specified in any other policies and procedures, such as those related to bringing your own device to the workplace.

[18] With respect to emails, the above-noted guidance document states the following:

> Custodians should develop and implement a written policy for sending and receiving personal health information by email. The policy should address when, how and the purposes for which this information may be sent and received by email, as well as any conditions or restrictions on doing so. The policy should also set out what types of information may be sent and received by unencrypted email and the circumstances in which the custodian will use unencrypted email.

[19] During this investigation, the clinic recognized that their practice was not in line with the above noted guidance. In response, the clinic committed to having all staff discontinue the practice of using personal emails for work-related purposes and to create business emails. The clinic has subsequently confirmed that business emails have been set up and staff are no longer permitted to use personal emails for work-related purposes.

[20] The clinic has also updated its email policy to reflect that staff are no longer permitted to use personal emails and advised staff about the new policy.

Shared Passwords:

[21] This complaint also raised a concern that clinic staff shared passwords to access

the clinic's systems. According to the clinic, at the time of the allegations its policy required, and continues to require, that every employee be given a unique user ID and customized password that they are required to use in order to access the clinic's Radiology Information System/Picture Archiving and Communications System (RIS/PACS). These systems have access to all patient data, appointments, as well as diagnostic testing, imaging and results. The patient data cannot be accessed without a specific user identification and password assigned to that user identification. The custodian advised that each staff member has a user identification and their own password.

[22] The clinic also has a policy titled "Secure identification of Users – RIS/PACS [name of business] Registration that addresses the secure identification of users. The document states that upon hire, every staff member will be given a username and password for the company's RIS/PACS. The document explains how to set up the secure login for the clinic's RIS/PACS system as well as advising that staff are not to share their login information with others. The document also advises staff that there is an audit trail set up in the RIS/PACS system and reminds all staff to log out of their work station when they walk away.

[23] In addition, upon hire the custodian advised that the Privacy Officer works with each staff member to ensure that they have been set up securely in the custodian's RIS/PACS system. The Privacy Officer also reminds each staff member directly that they are required to keep their username and password strictly confidential.

Passwords/Usernames Posted on the Computer

[24] Another concern raised in this complaint related to passwords and usernames posted on computers and visible to visitors of the clinic.

[25] In response to this concern, the clinic advised this office that their Privacy Officer completed a walk-through of the facility to determine whether any usernames and/or passwords were posted on or around computers.

[26] The Privacy Officer identified two computers with login information posted on the computer. The clinic advised that these logins were not RIS/PACS logins (the system that contains patient data) but logins to computers that allow the user to use Word and Excel programs. The clinic advised that no patient data is located on the two computers identified.

[27] In addition, the clinic advised that these two computers are not accessible to patients. The computers are located in offices with locked doors that are only accessible and utilized by interpreting physicians and administrative staff.

[28] Despite the above, the clinic advised that the notes identified were removed from the computers, the password logins were changed and the relevant staff were notified not to leave passwords on any computers.

System Security Patching, Virus Protection Software and Use of Windows 7:

[29] Lastly, this complaint raised concerns that the clinic did not complete system security patching, had insufficient virus protection software and alleged that some computers at the office used Windows 7, which the source of the complaint said is no longer supported by Microsoft and is therefore vulnerable to cyberattacks.

[30] The clinic denies the allegation that the system security patching was not occurring and there is insufficient virus protection software. The clinic confirmed that it has antivirus software in place on all clinic systems at all times.

[31] With respect to patching, the clinic advised that patches are done monthly and the clinic's Information Technology provider confirmed that all of its servers had been fully patched, with 100% of available patches applied.

[32] In addition, the clinic advised that it has had a manager firewall at the network level of its system, which is monitored, for approximately the last 14 years.

[33] Regarding the use of Windows 7 on clinic computers, the clinic explained that it has two computers that continue to have Windows 7 installed. The clinic advised that there is Bone Mineral Density software installed on the two computers and this software requires Windows 7. The clinic explained that the Bone Mineral Density software does not work with anything higher than Windows 7. The two computers that still run Windows 7 are not connected to the internet and are a closed system.

[34] The clinic also advised that the remainder of the computers were upgraded to Windows 10 in November 2019.

[35] In addition, as a result of this complaint, the clinic has contracted a cybersecurity consultant to complete an independent assessment of vulnerabilities in its technology infrastructure. The vulnerability assessment will cover the basic perimeter of the clinic's network (firewalls, routers, Wi-Fi networks, etc.), as well as Cloud and Outsourced IT services, websites and DNS records. A detailed report of cybersecurity threats that are discovered will be provided as well as a list of recommendations, security patches and upgrades that are required. The clinic has committed to implementing any of the recommendations, security patches and upgrades identified.

Privacy Training, Confidentiality Agreements and Audits:

[36] The clinic advised that staff are provided privacy training for data protection upon hire. In addition, whenever there are updates to the privacy legislation, the Privacy Information Officer provides this information to staff for review.

[37] Staff are also asked to review the clinic's privacy binder to ensure that they are aware of all the policies and procedures related to protecting personal health information.

[38] Moving forward, the clinic has agreed that in addition to the above, all staff will complete privacy training on an annual basis and the clinic will keep a record of the training completed and the date staff completed the training.

[39] During the investigation, the clinic advised that it requires all staff to sign confidentiality agreements upon hire, however, confidentiality agreements were not re-signed on an annual basis. Moving forward, all staff will re-sign confidentiality agreements on an annual basis and the custodian advised that it will keep a record of the signed agreements. Lastly, the clinic confirmed it completes privacy audits of its system on a monthly basis.

[40] This investigation file was opened in response to concerns raised about the adequacy of the clinic's privacy practices and administrative, technical and security measures in place. At the time the concerns were raised, the clinic's practice regarding staff's use of their personal email for business purposes, the posting/sharing of passwords and the lack of annual privacy training and re-signing of confidentiality agreements did not amount to adequate privacy practices, technical and security measures. I therefore find that at the time of this complaint, the clinic did not have reasonable measures in place to ensure the protection of personal health information against unauthorized disclosure as required by section 12(1) of the *Act*.

[41] However, in response to the complaint the custodian has created business emails, updated its policies to include that staff are no longer permitted to use personal emails for work-related purposes, confirmed that staff members have a unique user identification and password, reminded all staff to log out of their work station when they walk away, removed all notes from identified computers and changed relevant passwords, implemented annual privacy training and annual signing of confidentiality agreements and hired a cyber security consultant to complete an independent assessment of vulnerabilities in its technology infrastructure. The custodian has also committed to implementing any recommendations from the independent review. In light of the steps taken by the clinic, I am satisfied that the custodian has addressed the concerns in this complaint and now has adequate measures in place as is required by section 12(1) of the *Act*.

ISSUE 2: Is a review warranted under Part VI of the *Act*?

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

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

[43] In accordance with my delegated authority to determine whether a review is conducted under section 58(1) of the *Act*, and for the reasons set out above, I find that a review is not warranted.

NO REVIEW:

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

Original Signed by: July 5, 2022

Alanna Maloney
PHIPA Investigator