Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 205

Complaints HR20-00449 & HR21-00051

Health Service Providers

April 13, 2023

Summary: Two health service provider organizations, one a health information custodian (the Custodian), and the other an organization contracted to deliver health care services on behalf of the Custodian (the Agent), both reported the same privacy breach under the *Personal Health Information Protection Act, 2004 (the Act)* to the Information and Privacy Commissioner of Ontario (IPC). The breach involved a phishing email attack that resulted in the unauthorized use of personal health information relating to the Custodian's patients. However, in light of the steps taken by the Custodian and the Agent to address the breach, as well as the Agent's commitment to providing the IPC with an update before or by March 31, 2024 to confirm that the outstanding recommendations arising from the independent cybersecurity risk assessment that it undertook have been implemented, no formal review of the two complaints will be conducted under Part VI of the *Act*.

Statutes Considered: *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, sections 2, 3(1) 3, 4(1), and 12(1) and (2).

BACKGROUND:

[1] Two health service provider organizations, one a health information custodian (the Custodian) and the other an organization contracted to deliver health care services on behalf of the Custodian (the Agent), both reported the same privacy breach under the *Personal Health Information Protection Act* (the *Act* or *PHIPA*) to the Information and Privacy Commissioner of Ontario (the IPC or this office) that involved a phishing email attack.

[2] To address the breach, the IPC opened complaints HR20-00449 and HR21-00051 for the Custodian and the Agent, respectively.

HR20-00449 – Reported Breach by the Custodian

[3] The Custodian is one of multiple health service provider organizations that are related and provide health care services to individuals in their homes or in the community. At the time of the breach, the Custodian advised that the Agent was delivering health care services on behalf of these organizations under service provider contracts.

[4] The Custodian confirmed that it is a "health information custodian" and that the Agent is its "agent" under the *Act*. The Custodian explained that, for the purposes of delivering health care services on its behalf, the Agent collects, uses and discloses the personal health information (PHI) of the Custodian's patients and also processes their PHI in its data systems and facilities.

[5] The Custodian's breach report explained that, on June 1, 2020, its staff received a suspicious (phishing) email from the email account of an employee working for the Agent (the employee) which indicated that a privacy breach might have occurred.

[6] To contain the potential breach, the Custodian advised that its staff immediately reported the phishing email to its Information Technology (IT) department, who in turn quickly notified Ontario Health[1] and the Agent.

[7] Further, the Custodian advised that the employee's email account was blacklisted and blocked for both incoming and outgoing emails, and that its IT department issued an advisory to its staff in order to alert them to the phishing email. The Custodian explained that the advisory included details from the email, as well as a reminder not to click on the website link in the email (that led to a fraudulent website) and to report any further suspicious emails.

[8] The Custodian advised that, on June 2, 2020, Ontario Health confirmed that 286 people within the Ontario Health email system had received the phishing email and that almost all of the recipients were members of the Custodian's staff. As another containment step, the Custodian advised that Ontario Health stripped the redirect website link from the phishing email and manually blocked this website using their firewall rules. As a result, the Custodian advised that its staff was unable to access the website and, therefore, no logins, passwords or data on its network were compromised.

[9] Although the phishing email attack occurred on June 1, 2020, the Custodian

[1] The Custodian advised that Ontario Health provides it with electronic, health information network and IT services. In providing these services, the Custodian advised that Ontario Health also provides it with system security and protection. As such, the Custodian explained that it contacts Ontario Health as necessary, when issues such as system security, shut down access, or black list emails arise.

reported the incident as a breach to this office five months later in November 2020. The Custodian explained that the report was delayed because the Agent did not confirm that PHI relating to the Custodian's patients was affected by the attack until October 2020. Specifically, the Custodian advised that the Agent's review of the employee's email account found that it contained PHI relating to 373 patients for which the Custodian or one of its related organizations was a "health information custodian" under the *Act*.

[10] Further, the Custodian advised that the affected PHI included information relating to patients' names, allergies, diagnoses, medical reference numbers, medication, Ontario Health Insurance Plan numbers, policy account numbers, treating physicians and sensitive matters (defined by the Custodian as references to cancer, the human immunodeficiency virus and sexually transmitted infections).

[11] With respect to notification, the Custodian explained that of the 373 affected patients, it only considered 262 of them to be notifiable, that is, alive and able to be contacted. Regarding the other 111 affected patients, the Custodian advised that 45 of them were end of life and/or palliative patients for which notification was not clinically recommended in light of their vulnerability and that 63 of them were deceased with no executor contact information. For these 108 patients, the Custodian advised that a "note to file" about the breach was attached to their respective records. For the remaining three patients, the Custodian advised that they were unidentifiable due to missing key identifiers.

[12] To inform the affected patients that were notifiable of the breach, the Custodian advised that the Agent mailed 224 and 38 notification letters to them in January 2022 and November 2022, respectively.

[13] To remediate the breach, the Custodian advised that it worked with the Agent to better understand the form and extent of the PHI located in the employee's email account, the steps taken by the Agent to address the incident and, the robustness of the Agent's cybersecurity protocols and training.

[14] Regarding the preventive and protective measures that it is has in place to protect against cyberattacks, the Custodian advised that all incoming emails are scanned and that it has firewalls and controls which detect suspicious emails and strip redirects to (fraudulent) websites or attachments from their contents. The Custodian also advised that it often marks suspicious emails as potential spam in order to flag to the user that they should verify that the emails are authentic before opening their contents.

[15] In addition, the Custodian also advised that emails, even from known contacts and/or sources may also be marked as potential spam to notify the user to be cautious before opening them, and that other emails may be sent to junk mail folders and marked as potential spam to notify the user that they need to verify the legitimacy of the email.

[16] With respect to staff training, the Custodian advised that it provides them with specific training on phishing emails (e.g. what to do and how to report them) that includes phishing email examples and simulated phishing emails tests. Where an employee clicks on a test phishing email, the Custodian explained that they are followed up with and provided with corrective education and training. The Custodian also advised that its IT staff has cybersecurity expertise and training.

[17] Moreover, the Custodian confirmed that it has antivirus software installed on all of its hardware (i.e. servers, desktops and laptops), runs real-time scans and that its software and operating systems are regularly patched and updated.

[18] Regarding user privileges, the Custodian advised that it works on the least privilege required principle in the provision of accounts and granting access rights.[2] Moreover, regarding limited active content, the Custodian advised that it has controls in place to limit the ability to run scripts, executables or other code to only administrator accounts and that users are not set up with administrator privileges.

HR20-00051 – Reported Breach by the Agent:

[19] The Agent reported to this office that, on June 1, 2020, the Custodian advised it of the suspicious phishing email activity involving the employee's email account.

[20] To contain the incident, the Agent advised that it immediately initiated a password change to this email account in order to terminate any ongoing unauthorized access to PHI and instructed all internal recipients of the phishing email to also initiate an immediate password reset. The Agent also advised that it notified external recipients of the breach and instructed them to delete the phishing email immediately and contact their IT department if they had opened it.

[21] To investigate the potential breach and assist with remediation, the Agent advised that it retained a third-party forensic and cybersecurity expert (the cybersecurity expert).

[22] Regarding containment, the Agent advised that the cybersecurity expert confirmed the success of the password change in preventing any further unauthorized access to PHI. The Agent explained that, according to the cybersecurity expert, one of the malicious IP addresses used to distribute the phishing email was observed attempting to reauthenticate to the employee's email account unsuccessfully.

[23] Regarding the cybersecurity expert's investigation, the Agent advised they completed a thorough forensic investigation on the employee's email account and determined that the origin of the breach was a phishing email that the employee received from a trusted contact on March 10, 2020. The Agent also advised that the

[2] The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

investigation determined that the email account had been compromised and used to distribute approximately 2,000 phishing emails to both internal and external contacts.

[24] Further, the Agent advised that the cybersecurity expert determined that the phishing mail contained a link to a website with an embedded malicious file that was used to harvest Office 365[3] credentials, and that unknown actors with Internet Protocol (IP) addresses linked to the United Kingdom (UK) and Nigeria had accessed the employee's email account for a series of short intervals on March 14, 18, 19, 2020 and June 1, 2020.

[25] Regarding these intervals, the Agent advised that the cybersecurity expert determined the following:

- on March 14, 2020, the first instance of an unauthorized authentication occurred from an IP address originating from the UK and, shortly after authenticating, the unauthorized user moved the initial phishing email which led to the compromise to the account's "Deleted Items" folder;

- on March 15, 2020, authentications from three IP addresses originating from a mobile internet service provider in Nigeria were noted;

- on March 18, 2020, authentication from another IP address originating from the UK was noted, followed by evidence of calendar items and contact information being downloaded from the account;

- on March 19, 2020, authentication from the same IP address noted on March 18, 2020; and

- on June 1, 2020, a new IP address originating from the UK authenticated to the account and created an inbox rule to delete all incoming and outgoing mail from the account in preparation for the ensuing phishing campaign, and within minutes, phishing emails with a certain subject line or a similar variation thereof were sent to hundreds of internal and external contacts.

[26] Moreover, the Agent explained that the cybersecurity expert's investigation of these intervals included an analysis of forensic artifacts for indicators of data access or exfiltration. Regarding the outcome of this analysis and review, the Agent advised that the cybersecurity expert provided the following summary:

- activity conducted by the threat actor(s) was indicative of waging a phishing campaign, which provided the foundation to conduct a more widespread credential harvesting campaign;

---

[3] Office 365 is now Microsoft 365 which is a cloud-based productivity platform that include apps like Microsoft Teams, Word, Excel, PowerPoint, Outlook, and OneDrive. See https://www.microsoft.com/en-us/microsoft-365/microsoft-office.

- based on past use cases where the goal was data exfiltration (e.g., personal identifiable information or financial data), the following behaviour is commonly exhibited, which was not observed in this case:
    - where data exfiltration is a primary objective, there is commonly a higher level of mailbox interaction and data misuse, both of which were not identified in this case;
    - forwarding rules would send certain types of email to a rogue email account;
    - breach of a trusted relationship, where we observe conversations (internal or externally originating) inquiring about specific documents; and
    - overall, there's a higher level of interaction or different indicators found within the logs; and
- the totality of the incident suggests that of a security breach, rather than a breach of the mailbox itself, meant to harvest further credentials from other victims for a possible future campaign.

[27] With respect to the information affected by the breach, the Agent advised that the employee's email account held some form of health information for 2,942 individuals. However, the Agent explained that most of this information was in a non-consolidated and unidentifiable form such that it was not PHI.

[28] Regardless, out of an abundance of caution, the Agent advised that it undertook an extensive and systematic review of the contents of the email account and determined that, of the 2,942 individuals, 373 of them had PHI in an identifiable format and were patients of the Custodian or one of the Custodian's related organizations. The Agent also advised that it determined that the PHI of one of its patients, consisting of their name and a diagnosis, was affected by the breach.

[29] Regarding the PHI in the employee's email account, the Agent explained it would have required a rigorous search and review by the attacker(s) of the individual emails in the account in order to access this PHI and that there was no evidence of such activity.

[30] With respect to notification, the Agent advised that, on October 8, 2020, after the completion of the cybersecurity's investigation and despite having no reason to believe that PHI was accessed, copied or exfiltrated in the course of the phishing attack, it notified the Custodian of the outcome of the investigation and the steps that it took to contain and remediate the breach. The Agent also explained that it did not notify any affected individuals of the breach at the time because of this belief.

[31] However, in light of the direction that it received from this office during the

Intake Stage of the IPC's *PHIPA* complaint process[4] regarding notification, the Agent advised that, in January and November 2022, it sent notification letters to 262 patients of the Custodian who were affected by the breach and one of these letters to its affected patient.

[32] Regarding the preventive and protective measures that it is has in place to protect against cyberattacks, the Agent confirmed that it uses anti-virus technology on all end- points and data servers set to perform real-time scans and weekly deep scans of all servers. The Agent also confirmed that all of its devices, including mobile, server and laptop/desktop units, are updated with the latest software patches as soon as they become available. Moreover, the Agent advised that it is in the process of expanding the scope of its anti-virus service to perform rapid daily scans and weekly deep scans on all devices.

[33] Specifically, regarding email, the Agent advised that all of its email accounts and data servers are backed up on a daily basis in an environment segregated from its network. The Agent explained that the daily backups are then rolled into monthly and, ultimately, annual backups which are also stored off premises. The Agent also advised that backups are tested for viability every six months and that it has worked with a managed service provider to increase the frequency of disaster recovery testing on server backups.

[34] Further, the Agent advised that it places a banner on all emails from external sources warning the recipient of the potential for a phishing attack and that all incoming e-mails are scanned and assigned a point value based on their assessed potential for spam. The Agent explained that messages assigned a score below a certain threshold are delivered with a warning to the recipient of the potential for spam and that any attachments deemed to be malicious are filtered and not delivered.

[35] Regarding user privileges, the Agent advised that it underwent an independent cybersecurity risk assessment in 2020 and 2021 that produced 27 recommendations[5] of which 23 and 4 were classified as high and medium priority, respectively. The Agent confirmed that 20 of these recommendations have been implemented and that the remaining 7 recommendations will be implemented by or before March 31, 2024. As such, the Agent has committed to providing this office with an update by or before that date to confirm that these 7 recommendations have been implemented.

[36] Moreover, the Agent advised that common Office files with embedded macros are blocked and use native query warnings, and that it has worked on expanding its

---

[4] See the IPC's "Code of Procedure for Matters under the *Personal Health Information Protection Act, 2004"*.

[5] The recommendations relate to security awareness and education, adequate resources to mange cybersecurity processes, regular monitoring of user access logs, address gaps in security policies, restrict ability to download unauthorized software, regular reviews of user access privileges and security risk management, as well as other areas.

security protocols so that other file types will open with a text editor by default.

[37] With respect to remediation, the Agent advised that it has implemented the following measures to enhance the overall security of its electronic records and ensure that they are securely maintained and protected against cyberattacks:

- multi-factor authentication on all email and Office365 accounts;
- monthly access reviews of privileged accounts;
- additional security awareness training for employees, including training specific to phishing attacks;
- continuous vulnerability scans of servers and end-point devices;
- enacting recommendations from a recently completed independent cybersecurity assessment;
- using a security services vendor to provide vulnerability management and operational security support.
- an e-mail alert tool to report on phishing and other malicious correspondence;
- a security tool which scans uniform resource locator (URL)s and prevents access to malicious websites;
- enhanced security protocols for company mobile devices;
- utilizing Cisco Umbrella to manage end-point security;
- updated anti-virus technology; and
- enhanced firewall rules and signatures.

[38] Regarding staff training, the Agent advised that it implemented a cybersecurity awareness training program for all its employees in April 2022. The Agent explained that the program features, among other things, quarterly testing which is followed by active training via a Learning Management System on identification and responses to phishing attacks using simulated phishing emails.

[39] In addition to the aforementioned remedial steps, the Agent advised that it undertook the following measures:

- formulated a multi-year cybersecurity plan to address risks and recommendations arising from a recently completed independent risk assessment;

- selected a managed security service to support the Agent's cybersecurity initiatives and ongoing operational support;
- implemented a new Cybersecurity Incident Response Plan;
- assembled a Change Advisory Board with representation external to the organization with oversight over technological implementation and process controls; and
- revised workstation tool for enhanced end-point security.

ISSUES:

[40] There is no dispute that the Custodian is a "health information custodian", the Agent is an "agent" of the Custodian and that the privacy breach resulted in the unauthorized use of "personal health information" that was in the custody or control of the Custodian, all under the *Act*.

[41] Accordingly, as a preliminary matter, I find that:

- the Custodian is a "health information custodian" under paragraph 3 of section 3(1) of the *Act*;
- the Agent is an "agent" of the Custodian as defined in section 2 of the *Act*;
- the affected information that was in the custody or control of the Custodian and accessed by the attacker(s) without authorization contained "personal health information" within the meaning of section 4(1) of the *Act*; and
- as a result of the unauthorized access, this PHI was not protected against unauthorized use as required by section 12(1) of the *Act*.

[42] As such, this decision addresses the following issues:

1. Did the Custodian take reasonable steps to protect personal health information?
2. Did the Custodian notify the individuals affected by the unauthorized use of the personal health information in accordance with section 12(2) of the *Act*?
3. Is a review warranted under Part VI of the *Act*?

DISCUSSION:

Issue 1: Did the Custodian take reasonable steps to protect personal health information?

[43] In addition to having a privacy breach protocol in place, when a privacy breach occurs, this office has recommended that health information custodians immediately inform appropriate staff and identify the scope of the breach, take steps to contain, investigate and remediate the breach, and notify the affected individuals.[6]

[44] In this matter, as indicated above, both the Custodian and the Agent took all of these recommended steps. As such, the remainder of this discussion focusses on the practices that the Custodian has put in place to protect PHI as required by section 12(1) of the *Act*. 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.

[45] Further, pursuant to section 10(1) of the *Act*, custodians that have custody or control of PHI must "have in place information practices that comply with the requirements of this *Act* and its regulations." The term "information practices" is defined in section 2 of the *Act*, in part, as follows:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> …
>
> (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;

[46] This office has found that section 12(1) requires that health information custodians review their measures or safeguards from time to time to ensure that they continue to be reasonable in the circumstances to protect PHI in the custodians' custody or control.[7]

[47] Further, this office has stated that, in order to comply with the requirements in section 12(1) and to take steps that are reasonable in the circumstances to protect PHI,

---

[6] See the IPC's "Responding to a Health Privacy Breach: Guidelines for the Health Sector".
[7] Orders HO-010 and HO-013, PHIPA Decisions 64 and 70.

custodians must implement administrative and technical measures or safeguards, including privacy policies, procedures and practices, audit functionality, as well as privacy training and awareness programs and initiatives.[8]

[48] In this matter, to determine whether the Custodian has taken reasonable steps in the circumstances to ensure that PHI in its custody or control is protected against unauthorized use, the IPC's "Detecting and Deterring Unauthorized Access to Personal Health Information" and "Protect Against Phishing" guidance documents (the Preventing Unauthorized Access to PHI Guide and the Protect Against Phishing Guide, respectively) are informative [9].

[49] The Preventing Unauthorized Access to PHI Guide recommends that custodians implement the following measures to prevent or reduce the risk of unauthorized access:

- privacy polices and procedures;
- privacy training and awareness;
- privacy notices and privacy warning flags;
- confidentiality agreements;
- access management;
- logging, auditing and monitoring;
- privacy breach management; and
- discipline.

[50] The Protect Against Phishing Guide recommends that organizations adopt the following best practices to protect against phishing attacks:

- filter incoming messages;
- install malware detection and filters
- keep browsers and other software up to date;
- lock down workstations;
- require employees to use unique, complex passwords;
- identify external messages;

[8] Order HO-013.
[9] https://www.ipc.on.ca/wp-content/uploads/Resources/Detect_Deter.pdf and https://www.ipc.on.ca/wp-content/uploads/2019/07/fs-tech-protect-against-phishing-e.pdf

- segment networks that contain sensitive data from other networks;
- use threat intelligence and endpoint protection tools;
- by default, enable encryption on documents, devices and databases that contain sensitive information;
- conduct regular phishing awareness and training; and
- enable users to report phishing and to request help.

[51] This guide also recommends that organizations have a detailed incident response plan that sets out how the organization will respond to a suspected data breach or cyberattack.

The Custodian's Policies and Procedures

[52] As part of my investigation, I reviewed the Custodian's policies relating to privacy, unauthorized access to PHI, privacy incident and breach management, confidentiality, use of information & IT resources, as well as the Custodian's Guidelines For Determining Staff Sanctions For Privacy Breaches, training materials and other informational materials.

[53] Of note, the Custodian explained that all of its related organizations have similar policies, procedures, and training which are based on the *Act*, IPC guidance documents and the 10 privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information.

[54] The Custodian advised that its policies and materials are reviewed on an annual basis and whenever there may be an opportunity to update or provide clarity in the documents and/or training. The Custodian explained that these documents are made available to its staff through annual privacy and security training, which is tracked for compliance, and email phishing tests.

[55] The Privacy Breach Process for Unauthorized Access to PHI Policy sets out the corrective steps that designated staff members must take to address and resolve a privacy breach relating to unauthorized access. Further, the Privacy Incident and Breach Management Policy applies to all of the Custodian's employee and agents and provides direction "regarding appropriate management of privacy incidents and breaches, and to indicate the actions and steps to be undertaken to contain, resolve and investigate incidents and breaches in a timely and efficient manner."

[56] The Privacy Policy sets out the principles that have been implemented by the Custodian to meet its privacy obligations under the *Act*. This policy covers PHI in the Custodian's custody or control and requires that all of its employees and agents adhere to it.

[57] Further, the Privacy Policy provides that "…[PHI] will be protected by security safeguards appropriate to the sensitivity of the information" and that methods of protection include "administrative measures such as policies and procedures to protect the privacy and security of [the Custodian's] data holdings" and "technical measures such as the use of passwords, encryption, firewalls, and other technical security safeguards."

[58] With respect to email, this policy prohibits the sending of email messages containing PHI to an external email account unless approved by the Custodian's Privacy Officer, and that "internal use of email related to patients should be limited, but is acceptable as long as personal identifiers are removed."

[59] Regarding staff discipline, the Privacy Policy provides that where an employee violates this policy, they may be subject to disciplinary action, up to and including termination of employment. Further, the Custodian's Guidelines For Determining Staff Sanctions For Privacy Breaches defines four levels of a privacy breach – (1) inadvertent access or disclosure, (2) negligence, (3) curiosity, concern, deliberate act and (4) personal gain, malice, repeated offences – to help guide corrective and disciplinary action.

[60] The Confidentiality Policy applies to all of the Custodian's employees and agents, and requires that they ensure the confidentiality of PHI and not disclose this information to any unauthorized persons. This policy also requires that all of the Custodian's employees and agents sign an Agreement of Confidentiality on or before their first day of work and makes it clear that a violation of confidentiality may result in disciplinary action up to and including dismissal, as well as the reporting of the offender to their regulatory college where applicable.

[61] The Use of Information & Information Technology Resources Policy defines the security requirements and best practices relating to the use of the Custodian's information and IT resources. This policy applies to all of the Custodian's employees and agents, and its scope encompasses desktop computers, laptop computers, handheld devices, servers and all portable storage media.

[62] The objective of the Use of Information & Information Technology Resources Policy "is to ensure that use of I&IT resources does not result in unacceptable risks to [the Custodian] and that the privacy and security of personal information and [PHI] is appropriately protected." This policy also sets out procedures relating to education and training, security of the Custodian's IT resources, systems monitoring, personal monitoring, password management, remote access, mobile devices, reporting privacy and security incidents and unacceptable use of information and IT resources (e.g. email messages).

[63] My review of the training and information materials that the Custodian provides to its employees define cybersecurity, explain the dangers of cyberattacks and how they

occur, and outline cybersecurity tips for remote work. These materials also provide guidelines for establishing a secure Wi-Fi network, creating strong passwords, using virtual private network, protecting confidential information, protecting personal devices and protecting against phishing. Further, these materials explain the importance of privacy, confidentiality and security with respect to the *Act*.

The Agent's Policies and Procedures

[64] As part of my investigation, I reviewed the Agent's policies relating to privacy event management, privacy, confidentiality, information security, email security, end-user training, firewall protection, remote access, as well as the Agent's Cyber Incident Response Plan, training materials and other informational materials.

[65] The Agent advised that its policies and materials are reviewed every two years, and that these documents are available to its employees at all times through its Intranet site. The Agent also advised that all of its new hires are required to complete privacy training within 90 days of their start date, and that all of its employees are required to review the polices, as well as reaffirm their confidentiality pledge, on an annual basis.

[66] The Privacy Event Management Policy sets out the guidelines and procedures to be followed in response to a privacy breach and covers privacy incidents relating to emails and PHI that is accessed without authorization. Moreover, the Cyber Incident Response Plan sets out the Agent's response to cyber incidents and, more specifically, "documents the roles and responsibilities and steps that will be followed to identify, contain, eradicate, communicate and recover from cyber incidents. Steps include Preparation, Identification, Containment, Eradication, Communications, Recovery and Lessons Learned."

[67] The Privacy Policy prohibits the unauthorized use of PHI and makes the Agent accountable for all PHI in its care. This policy requires that the Agent implement security safeguards to protect PHI against unauthorized access where such methods of protection include physical, organization and technological measures. In addition to the safeguards relating to email mentioned above, the Agent also advised that it also uses DuoCircle, a technology which provides inbound e-mail filtering to reduce the amount of spam, phishing campaigns and unwanted e-mails, as well as URL rewriting, a technology which allows an organization to track users who may have clicked on malicious URLs.

[68] The Confidentiality Policy requires that the Agent's employees keep PHI confidential. This policy also provides that a privacy breach "caused by deliberate, repeated or carless action is subject to disciplinary action up to and including termination with cause." Moreover, it sets out safeguards to be taken in order to ensure that PHI remains confidential.

[69] Under the Information Security Policy, the Agent acknowledges that it has obligations to protect PHI as defined under the *Act*. This policy applies to all of the Agent's employees and was made in alignment with the National Institute of Standards and Technology's Cybersecurity Framework which provides guidance based on existing standards, guidelines and practices to help organizations better manage and reduce cybersecurity risk.[10]

[70] With respect to email, the Email Security Policy requires that Agent have processes and controls "in place to ensure that the risk presented by email systems and email messages with respect to loss, disclosure, or damage to [its] network or data is minimized." Further, this policy prohibits the Agent's employees from opening an email message that is received from an unfamiliar source and that such emails are immediately deleted and purged, unless there is evidence to indicate that they are legitimate, as well as be thoroughly investigated before it is opened to determine the source and objective of the email.

[71] The End-user Training Policy requires that the Agent have processes and controls in place to ensure that its staff have appropriate training and technical support for all of its IT resources. Specifically, this policy requires that the Agent's staff be provided with:

- IT orientation materials identifying and documenting the IT services and systems available;
- information regarding education options available for each service, including a timetable for training sessions provided by IT Technical Support or third-party training providers; and
- help desk information, including hours of availability and contact information.

[72] The Firewall Protection policy requires that the Agent "have firewall protection installed and configured to limit network traffic to only those protocols required for business processes." Further, the Remote Access Policy stipulates that the Agent may implement remote access mechanisms to its internal systems, networks and data only if such access "can be justified to achieve a business or operational goal" and it "can be implemented with sufficient security to minimize the risks of exposing company systems, networks and data."

[73] To ensure that staff are educated and trained with respect to phishing attacks, the training materials that the Agent provides to its employees give instruction on how to report phishing emails. In addition, the Agent's informational materials relating to viruses, worms and malware, inform its employees of possible malware infestation symptoms, describes the various types of malware and confirms that the Agent will implement several layers of defences to protect against cyberattacks.

---

[10] https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide.

Analysis

[74] The Custodian believes that it complied with section 12(1) of the *Act* based on the information practices, as well as the administrative, technical and physical safeguards that it and the Agent had in place at the time of the breach. Further, the Custodian advised that it maintains this position because, as indicated above, the phishing email attack did not result in unauthorized access to the affected PHI through its email system.

[75] Moreover, the Agent explained that it complied with section 12(1) because, as indicated above, the root cause of the breach was determined to be theft of valid user credentials by way of a phishing email that the employee received from a trusted contact whose account had presumably also been compromised at that time. As a result, the Agent advised that, in its view, the breach was due to human error which no organization can fully prevent.

[76] For these reasons, and based on my review of the Custodian and the Agent's information practices in place at the time of the breach which appear to be in accordance with the recommendations found in the Preventing Unauthorized Access to PHI Guide and the Protect Against Phishing Guide, I am satisfied that the Custodian took reasonable steps in the circumstances to ensure that PHI in its custody or control was protected against unauthorized use as required by section 12(1).

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

[77] Section 12(2) of the *Act* requires that health information custodians notify individuals whose PHI is used without authorization. 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.

[78] With respect to notifying individuals, the IPC's "Responding to a Health Privacy Breach: Guidelines for the Health Sector" is informative. This guidance document recommends that individuals that are affected by a breach be provided with the following information:

- the date of the breach;
- the description of the nature and scope of the breach;
- a description of the PHI that was subject to the breach;
- the measures implemented to contain the breach, and
- the name and contact information of the person in your organization who can address inquiries.

[79] Based on my review of the notification letter that was sent to the affected individuals, I am generally satisfied that it contained the recommended aforementioned information.

[80] In this matter the phishing email attack occurred in June 2020, and in October 2020, the Custodian became aware that its patients' PHI had been affected by the breach. However, these affected individuals were not notified until January and November 2022. Therefore, the Custodian took over one year to notify them.

[81] Regarding the notification delay, the Custodian explained that, because the PHI in the employee's email account was primarily in non-consolidated and unidentifiable form, it took some time to identify the medical and treatment status for the affected individuals. Moreover, the Custodian explained that it (mistakenly) took the view that notification was not required based on the Agent finding no evidence that the affected PHI was accessed, copied or exfiltrated.

[82] Although it may have taken the Custodian some time to identify which individuals were affected by the breach, in my view, once this determination was made in October 2020, these individuals should have received notification at that time. In my view, this would have been the first reasonable opportunity to do so, as the Custodian (and the Agent) did not provide any other evidence to suggest or demonstrate why notification could not have been provided to the affected individuals then.

[83] For these reasons, I find that the Custodian did not provide its patients affected by the breach with the notification required by section 12(2) of the *Act*. That is, I find that the Custodian did not provide notice of the breach "at the first reasonable opportunity" as required by this section.

[84] In response to this finding, as a remedial step, the Custodian confirmed that it is committed to providing notification to its patients in accordance with section 12(2). The Custodian also advised that, as a result of the breach, it has modified its processes in order to increase the efficiency of its notification process. To that end, more specifically, the Custodian advised that its notification process now includes notice being controlled and provided by the Custodian directly, rather than by the Agent, once the affected patients and the PHI involved are identified. As a result, the Custodian confirmed that it

will no longer delegate notification duties to the Agent.

[85] For these reasons, despite my finding above, I am satisfied that the Custodian has taken adequate steps to address the notification delay that occurred in this matter.

Issue 3: Is a review warranted under Part VI of the *Act*?

[86] 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.

[87] 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.

DECISION:

For the foregoing reasons, and as the Agent has committed to providing this office with an update before or by March 31, 2024 to confirm that the seven outstanding recommendations arising from the independent cybersecurity risk assessment that it undertook have been implemented, no review of the two complaints will be conducted under Part VI of the *Act.*

Original signed by: April 13, 2023

John Gayle
PHIPA Mediator/Investigator