Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 255

File HR22-00297

Simcoe Muskoka District Health Unit

July 5, 2024

Summary: In July 2022, the respondent Simcoe Muskoka District Health Unit (SMDHU) was the subject of an email phishing attack. As a result of the attack, a threat actor gained access to one SMDHU email account containing approximately 20,000 emails, including about 1,000 emails containing personal health information. SMDHU reports that the threat actor's access to the compromised email account was limited to one hour, and that its forensic analysis found no evidence that the threat actor viewed, downloaded, copied, sent, forwarded, or removed any emails while in the compromised account.

The IPC initiated a review of the matter under the *Personal Health Information Protection Act, 2004* (*PHIPA*). Section 12(2) of *PHIPA* sets out a duty on health information custodians like SMDHU to notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or used or disclosed without authority. SMDHU asserts that there is no evidence to conclude, on a balance of probabilities, that any such privacy breach occurred, and on this basis takes the position that the duty to notify does not apply.

In this decision, the adjudicator concludes, on a balance of probabilities, that the threat actor's undisturbed access to an SMDHU email account containing a considerable amount of personal health information resulted in both an unauthorized disclosure and an unauthorized use of personal health information. As a result, the duty to notify in section 12(2) applies. During the IPC review, SMDHU decided to send detailed letter notices to individuals whose personal health information may have been affected by the phishing attack. The adjudicator finds that through its direct notification of individuals during the review, SMDHU provided notice as required by section 12(2) of *PHIPA*, although it should have done so at the first reasonable opportunity. In the circumstances, she concludes the review without issuing an order.

Statutes Considered: *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Sch A, sections 2 (definitions), 3(1), 12(1) and (2), 29, and 58(1); General, RRO 1990, Reg 460 under the *Freedom of Information and Protection of Privacy Act*, section 4(1); General, RRO 1990, Reg 823 under the *Municipal Freedom of Information and Protection of Privacy Act*, section 3(1).

Decisions Considered: PHIPA Decisions 49, 110, and 210.

OVERVIEW:

[1] This decision and three other decisions that I am issuing on this date[1] consider different situations involving cyberattacks on organizations subject to the *Personal Health Information Protection Act, 2004* (*PHIPA*) and Part X of the *Child, Youth and Family Services Act, 2017* (*CYFSA*). These statutes require covered organizations to take reasonable steps to protect the security of individuals' personal health information (or personal information under the *CYFSA*) in their custody or control, including against theft, loss, and unauthorized use or disclosure. They also require the notification of affected individuals at the first reasonable opportunity if such a privacy breach occurs.

[2] In each of these decisions, I consider whether the cyberattack at issue resulted in a theft, loss, or unauthorized use or disclosure of individuals' personal health information or personal information, so that the relevant duty to notify applies. As these decisions illustrate, a cyberattack on an organization's information systems may trigger the duty to notify whether or not the attacker takes further malicious action (like using stolen identity information, or demanding a ransom) with the affected information. These decisions also demonstrate that the duty to notify can be met in different ways. In determining the appropriate form of notice, organizations should consider relevant circumstances, including the adequacy of the response to the cyberattack, the volume and sensitivity of the affected information, and evidence of any continuing privacy risks from the attack.

[3] This decision concerns an email phishing attack on the Simcoe Muskoka District Health Unit (SMDHU), a health information custodian within the meaning of *PHIPA*.[2] For the reasons that follow, I find that a threat actor's unauthorized access to an SMDHU email account containing personal health information resulted in an unauthorized disclosure and an unauthorized use of personal health information within the meaning of section 12(2) of *PHIPA*. As a result, SMDHU had a duty to notify affected individuals at the first reasonable opportunity. During the IPC review, SMDHU sent detailed letters notifying individuals whose personal health information may have been affected by the breach. I find that through these letters, SMDHU provided notice as required by section 12(2), although it should have done so much earlier. In the circumstances, I conclude the review without making an order.

---

[1] PHIPA Decisions 253 and 254, and CYFSA Decision 19.

[2] Specifically, the medical officer of health of the board of health governing SMDHU is the health information custodian (paragraph 6 of section 3(1) of *PHIPA*).

BACKGROUND:

[4] On July 20, 2022, a number of SMDHU employees received phishing emails from an external partner's business email address. A phishing email is a type of online attack designed to trick the recipient into revealing sensitive information or downloading malicious software.[3] The majority of SMDHU employees notified the IT department of the suspicious email shortly after receipt. However, one employee opened the link contained in the phishing email and provided his SMDHU email access credentials, including a multi-factor authentication code, to the unknown third party (the threat actor), compromising the email account.

[5] When SMDHU's IT department became aware of the phishing attack, it immediately removed the emails from SMDHU email systems and initiated a mandatory password reset. Because of this action, the threat actor was expelled from the compromised email account about one hour after gaining access and was unable to regain access, although it made multiple attempts to do so.

[6] The compromised email account contained approximately 20,000 emails dating to 2010, including approximately 1,000 emails containing personal health information, primarily in the form of vaccination statuses and exemptions for adults and minors. SMDHU's forensic investigation found that the threat actor had logged into the compromised account via a web application, which would have prevented the threat actor from mass-downloading any emails or attachments contained in the compromised account. SMDHU's investigation also determined that the threat actor had not sent or forwarded any emails from the compromised account.

[7] Based on this information, SMDHU reported the phishing attack to the Office of the Information and Privacy Commissioner of Ontario (IPC), but took the position that the evidence did not support a finding, on a balance of probabilities, that personal health information had been stolen, lost, or used or disclosed without authority. The IPC opened the present file to address this matter.

[8] At the early resolution stage of the IPC process, IPC staff sought and received updates from SMDHU about the phishing attack, including about the nature and scope of the attack, the actions taken by SMDHU to investigate and to respond to the attack, and SMDHU's cybersecurity practices more broadly. SMDHU worked cooperatively with the IPC to provide this information. By the end of the early resolution stage, IPC staff were satisfied with SMDHU's investigation and containment efforts. Those aspects of SMDHU's response to the phishing attack are not at issue in this review.

[9] However, this matter proceeded to adjudication to address outstanding issues arising from SMDHU's position that the phishing attack did not give rise to the duty in

[3] IPC Technology Fact Sheet, "Protect Against Phishing" (July 2019). Available online: https://www.ipc.on.ca/.

section 12(2) of *PHIPA* to notify affected individuals. I decided to conduct an IPC-initiated review of this matter under section 58(1) of *PHIPA*. Section 58(1) permits the IPC to conduct a review of any matter, on its own initiative, where it has reasonable grounds to believe that a person has contravened or is about to contravene a provision of *PHIPA* or its regulations.

[10] During the review, I sought and received representations from SMDHU on whether the phishing attack resulted in the theft, loss, or unauthorized use or disclosure of personal health information, within the meaning of those terms in section 12(2) of *PHIPA*, and, if so, the appropriate form of notice in the circumstances.[4]

[11] SMDHU has asked that I withhold details of its security safeguards, including the brand names of software and devices, based on a concern that sharing these details publicly could put SMDHU at an increased risk of future cyberattacks. I accept this request, and in this decision I have wherever possible left out references to the specifics of SMDHU's security safeguards.[5]

ISSUES:

A. Does the notification requirement in section 12(2) of *PHIPA* apply in the circumstances?

B. If the duty to notify applies, was notice given in compliance with section 12(2)?

DISCUSSION:

[12] Among other purposes, *PHIPA* sets out rules to ensure the security of "personal health information" that is in the "custody" or "control" of a health information custodian.[6]

[13] As a preliminary matter, SMDHU agrees that: 1) it is a health information custodian; 2) the compromised email account contained personal health information; and 3) this personal health information was in SMDHU's custody or control, within the

---

[4] I also asked SMDHU to comment on the potential relevance to my review of IPC Orders HO-004 and HO-007. In those orders, the IPC endorsed the strong encryption of mobile devices as a potentially effective means of mitigating the risks associated with having personal health information accessed outside normal network protections. While SMDHU provided supplementary representations on this topic at my request, I ultimately concluded that there are significant factual differences between the circumstances present in those IPC orders and the matter before me. Those orders are not relevant here, and I have not relied on them in making my determinations in this decision.

[5] In doing so I follow the approach taken in PHIPA Decision 210 (at para 7).

[6] The term "personal health information" is defined in section 4 of *PHIPA*. "Custody" and "control" are not defined in *PHIPA*. However, the IPC has interpreted these terms in *PHIPA* in a manner consistent with the IPC's broad and liberal approach to interpreting these same terms in *FIPPA* and its municipal counterpart, the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), and in the *CYFSA*: see PHIPA Decision 232, among others.

meaning of those terms in *PHIPA*. There is no dispute that *PHIPA* applies to the personal health information at issue in this review.

A. Does the notification requirement in section 12(2) of PHIPA apply in the circumstances?

[14] Section 12(1) of *PHIPA* sets out obligations on health information custodians to take reasonable steps to protect the security of personal health information in their custody or control. 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.

[15] The duty to take reasonable steps to protect personal health information includes a duty to respond promptly and adequately to a privacy breach. Among other things, a proper response will help to ensure that any privacy breach is contained and will not re-occur.

[16] A proper response also includes notifying any individuals whose personal health information is affected by a privacy breach, in accordance with section 12(2). This section states:

> Subject to subsection (4) [which is not applicable in the circumstances of this file] 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.

[17] SMDHU says that the language of section 12(2) (i.e., the present verb tense in the phrase "is stolen or lost or … is used or disclosed without authority …") indicates that the duty to notify requires a factual finding, made on a balance of probabilities, that personal health information was actually stolen or lost, or actually used or disclosed without authority. It submits that *PHIPA* does not require custodians to notify individuals of potential or possible or speculative events, or of mere vulnerabilities in a system. SMDHU notes that an overly broad interpretation of the duty to notify could invite unintended and unwanted consequences, like notification fatigue on the part of the public and undue

costs to the custodian.

[18] I agree with SMDHU that the duty to notify in section 12(2) does not arise where there is a mere potential or possibility of a privacy breach. I agree that the duty to notify arises from a finding, made on a balance of probabilities, that one of the events described in section 12(2) has occurred.

[19] In the discussion that follows, I explain why I find, on a balance of probabilities, that the phishing attack on SMDHU's email systems resulted in both an unauthorized disclosure and an unauthorized use of personal health information in SMDHU's custody or control.[7]

The phishing attack resulted in an unauthorized "disclosure" and unauthorized "use" of personal health information within the meaning of section 12(2)

[20] The terms "disclose" and "use" are defined in section 2 of *PHIPA*, as follows:

> "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[.]
>
> "use", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to view, handle or otherwise deal with the information, subject to subsection 6 (1),[8] but does not include to disclose the information, and "use", as a noun, has a corresponding meaning.

[21] Section 29 of *PHIPA* applies to any collections, uses, and disclosures of personal health information by health information custodians. Under this section, *PHIPA* authorizes the use and disclosure of personal health information in some circumstances—namely, where there is the appropriate consent (and other conditions are met); or where *PHIPA* permits or requires the use or disclosure to be made without consent.

[22] If a use or disclosure occurs outside these circumstances, then that use or disclosure is not authorized under *PHIPA.* In such a case, the personal health information will have been "used or disclosed without authority" within the meaning of section 12(2), and the duty to notify will be triggered.

---

[7] Because of my findings in this decision, it is unnecessary for me to decide whether the phishing attack at issue in this review also qualifies as a theft and/or a loss of personal health information within the meaning of section 12(2), and I decline to do so.

[8] Section 6(1) of *PHIPA* clarifies that the providing of personal health information between a custodian and its agent is also a "use" of that information (and not a disclosure by the custodian and corresponding collection by the agent).

[23] In explaining why it believes the duty to notify does not apply in this case, SMDHU cites the following findings from its investigation of the phishing attack:

- The threat actor had only one hour of access to one compromised email account;
- The threat actor logged into the compromised email account using a web application, which by design prevents the mass-downloading of emails or attachments in the compromised account;
- SMDHU never lost access to the inbox associated with the compromised email account or the information contained within that account;
- The threat actor did not send or forward any emails while in the compromised email account; and
- The threat actor did not create any email account rules to automatically send or forward emails from the compromised email account.

[24] SMDHU acknowledges that it is not possible to know whether the threat actor engaged in certain activities (like searching the inbox, or viewing or opening any particular email) while it was inside the compromised email account. Nonetheless, SMDHU says, the available evidence does not a support conclusion, on the balance of probabilities, that the personal health information of specific individuals was stolen, lost, or used or disclosed without authority.

[25] I accept SMDHU's statement that it may never be possible to say with certainty what activities the threat actor engaged in while inside the compromised account. In the circumstances, however, I am satisfied, on a balance of probabilities, that the threat actor's unauthorized access to an SMDHU email account resulted in both an unauthorized disclosure and an unauthorized use of personal health information, within the meaning of those terms in *PHIPA*.

Disclosure

[26] I find that the threat actor's infiltration of an SMDHU email account containing unencrypted[9] emails of personal health information qualifies as a "disclosure" of that information within the meaning of *PHIPA*. This is the case even accepting SMDHU's assertion that there is no evidence the threat actor further disclosed (for example, by downloading or forwarding) any personal health information contained in the compromised account. As noted above, the definition of "disclose" in *PHIPA* includes the act of making personal health information available to another person. When the threat

[9] During the review, SMDHU provided detailed information about its security safeguards (including encryption) for emails and attachments stored at rest in and sent between SMDHU email accounts. As SMDHU explained, however, once a user authenticates to an email account (as the threat actor did here, through valid credentials fraudulently obtained through the phishing attack), the contents of the email account are no longer encrypted to that user.

actor gained access to an SMDHU email account (through fraudulently obtained user credentials), SMDHU effectively shared with or exposed to (i.e., in the language of *PHIPA*, "made available" or "released" to) the threat actor personal health information in that account.

[27] I acknowledge that this disclosure of personal health information occurred despite SMDHU's lack of intention, or even awareness, with respect to the threat actor's unauthorized activities. I accept SMDHU's assertion that its intention was in fact the opposite—namely, to preclude unauthorized access, including by threat actors, as evidenced by the security safeguards SMDHU had in place to protect its email systems.

[28] SMDHU asserts that the intention of the disclosing party is key. It says that the text of *PHIPA* indicates that a custodian does not disclose personal health information when it unintentionally makes that information available to an unauthorized person. SMDHU also says that the phrase "to make [personal health] information available or to release," in *PHIPA*'s definition of "disclose," indicates that there must be an action by the custodian, rather than inaction or neglect, to qualify as a disclosure. SMDHU proposes that had the Legislature intended for data exposure associated with a security incident to qualify as a disclosure, it would have used the words "to fail to protect" in the definition of disclose.

[29] I disagree. As I will explain, I see no basis in *PHIPA* to read into the definition of "disclose" SMDHU's proposed requirements of intention and positive action by the disclosing party.

[30] During the review, I invited SMDHU to comment on the potential relevance of some IPC decisions involving situations of covert and unauthorized accesses by third parties to personal health information in a custodian's custody or control. PHIPA Decision 49 involved a patient who was left unsupervised in a doctor's office and who took photographs of a computer screen displaying the personal health information of other patients. PHIPA Decision 110 involved agents of custodians who were authorized by the custodians to access shared electronic medical records systems, but who, in specified instances, improperly viewed the records of family members, acquaintances, and other individuals without an authorized purpose in *PHIPA* for doing so. I noted that in these decisions, the IPC concluded that the custodian had "disclosed" personal health information within the meaning of *PHIPA*, by releasing or making available that information to an unauthorized third party, despite the custodian's lack of intention to share that information with the unauthorized party.

[31] SMDHU acknowledges that in these cases, the IPC found that the custodian improperly disclosed personal health information to the parties who improperly accessed that information. However, SMDHU says, these cases involved a positive action by the custodian—for example, the custodian's errant displaying of personal health information in PHIPA Decision 49, and, in PHIPA Decision 110, the custodians' initial granting of permissions to their agents to access their electronic records systems for authorized

purposes. SMDHU says the situation before me is different, in that there was no act by which SMDHU failed to protect personal health information under its control (for example, it did not errantly display that information), and there was no intention on the part of SMDHU to give the threat actor access to SMDHU email accounts.

[32] I find unpersuasive these distinctions proposed by SMDHU. On the factual matter of whether a custodian made available or released personal health information to another party, I agree with and adopt the IPC's previous findings that the intention of the custodian (either with respect to the disclosure itself, or the means by which the disclosure is made possible) is irrelevant.[10]

[33] Additionally, I see no basis for SMDHU's proposal to limit the definition of disclosure to positive acts performed by a custodian. It is my view that a purposive interpretation of the term in section 12(2) captures not only positive and intentional actions, but also unintentional actions, as well as inaction or neglect, where that action or inaction results in an unauthorized "making available" of or "release" of personal health information in a custodian's custody or control. By contrast, SMDHU's proposed definition would treat differently the same unauthorized release of personal health information, depending on whether it arises from an intentional, positive action or from an unintentional action, or neglect.

[34] Consider the example of a burglar who breaks into a doctor's office and views patient files without authority (but who does not steal or otherwise remove those files from the doctor's office). Under SMDHU's proposed interpretation, there would be a duty to notify patients of the unauthorized exposure of their personal health information only if the doctor's office intended for the break-in to occur, and performed some positive action to allow the burglar's access. By contrast, there would be no duty to notify where the break-in and unauthorized viewing of patient files occurred without any intention or positive action on the part of the doctor's office. I see no principled reason why the duty to notify should apply in the former case, but not in the latter.[11]

---

[10] See, for example, PHIPA Decision 49, at paragraph 41: "What is clear is that the Respondent took a photo of a computer screen at the doctor's office. In these unique and unusual circumstances, I am satisfied that the personal health information at issue was 'made available' to the Respondent by the Physician. I accept that this was done inadvertently and in error, and that there was no intention to make the information available to the Respondent. However, the fact is that the Respondent was able to take a photo of the information while attending at the Physician's office, and that the Physician, as the health information custodian with custody or control of this personal health information, displayed this personal health information to the Respondent. In these circumstances, I am satisfied that the Physician made this information available, and thereby disclosed personal health information to the Respondent…"
Also see paragraph 72 of PHIPA Decision 110: "It is irrelevant to this analysis that THP may have had no intention to provide to the physicians' agents any personal health information that the agents were not authorized under *PHIPA* to collect. The definition of 'disclose' in *PHIPA* merely requires that THP make available or release personal health information in its custody or control, which THP did by giving the physicians and their agents permissions to access its EMR."

[11] As an aside, I note that one could characterize as a positive action the SMDHU employee's act of providing his email user credentials to the threat actor.

[35] Beyond these main arguments, SMDHU reiterates its concern that an overly broad interpretation of section 12(2) could result in notification based on the mere potential for harm, rather than a factual finding that an unauthorized activity (such as unauthorized disclosure) has occurred. It argues that the duty to notify does not arise based on the mere potential for browsing or downloading personal health information. It offers the following analogy: "To say that SMDHU made [personal health information] available to the [threat actor] is to say that an otherwise physically secure hospital that is nevertheless broken into has made all information in every file cabinet available to the burglar."

[36] The situation before me involves a threat actor's unauthorized access to an email account containing significant amounts of unencrypted personal health information—i.e., access to the very location holding personal health information. A more apt analogy than the one offered by SMDHU would be a burglar's unauthorized access to the very room in the hospital in which unsecured files of patient personal health information are stored.

[37] As noted above, I share SMDHU's view that the duty to notify in section 12(2) does not arise based on a mere potential or possibility of a privacy breach. I agree that the duty to notify is triggered where there is a finding, made on a balance of probabilities, that one of the events described in section 12(2) has occurred. It is my finding in this case that the threat actor's infiltration of an SMDHU email account containing unencrypted personal health information, and the resulting availability to the threat actor of that information, satisfies the plain words of the definition of disclosure in *PHIPA*. On the analogy offered by SMDHU, I note only that I see no statutory impediment to finding, on a balance of probabilities, that a disclosure occurs in circumstances where a third party's unauthorized entry into an otherwise physically secure location makes available to the third party personal health information in the custodian's custody or control.

[38] For these reasons, I find that the threat actor's infiltration of an SMDHU email account resulted in a disclosure of personal health information by SMDHU to the threat actor. There is no claim that this disclosure occurred with the appropriate consent, or was permitted or required to be done without consent under *PHIPA*. In these circumstances, the disclosure was not authorized by *PHIPA*.

Use

[39] I also find that the threat actor's infiltration of the SMDHU email account containing personal health information resulted in a "use" of personal health information within the meaning of *PHIPA*. This is because I am satisfied, on a balance of probabilities, that the threat actor viewed, handled, or otherwise dealt with personal health information contained in the compromised account.

[40] SMDHU asserts that "the same facts cannot satisfy the definition of 'disclose' and 'use,'" and that, as a result, the threat actor's unauthorized access to the compromised email account "cannot be, at once, a use and a disclosure." I understand SMDHU to be referring to the following part of the definition of disclose in *PHIPA* (emphasis mine):

> "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[.][12]

[41] The distinction made here is in keeping with *PHIPA*'s different rules concerning a party's uses and disclosures of personal health information. I do not read these caveats in the definitions of "disclose" and "use" to preclude a finding that a disclosure of personal health information by one party can lead to a use *by a different party* of the same information. It is logically coherent that a disclosing party's "making available" or "release" of (i.e., disclosure of) personal health information to a receiving party is a corresponding "handling" of or "dealing with" (i.e., use of) that same information by the receiving party. I am thus not persuaded of any statutory or other impediment to finding that an event that results in a disclosure of personal health information by SMDHU to the threat actor also results in a use by the threat actor of the information disclosed to it.

[42] SMDHU's more significant argument has to do with its view of whether the evidence in this case supports a finding, on a balance of probabilities, that the threat actor "used" personal health information in the compromised email account.

[43] SMDHU says that the threat actor's unauthorized access to an email account containing personal health information is not, by itself, direct evidence that the threat actor actually viewed any individual email of personal health information inside the compromised account. It notes that when an authorized user logs into an email account, that user does not as a result "view" every email contained in that account; instead, the user must open or preview an email to view its contents. SMDHU maintains that in the absence of evidence that the threat actor actually viewed any particular email of personal health information, it is not possible to say, on a balance of probabilities, that the threat actor used personal health information within the meaning of section 12(2).

[44] I arrive at a different conclusion, based on my assessment of the circumstances of the breach.

[45] There is no dispute that following its successful phishing attack, the threat actor had access, for one hour, to an SMDHU email account containing over 1,000 unencrypted emails of personal health information. I accept that it may not be possible to say with certainty which particular emails of personal health information, if any, the threat actor viewed, handled, or otherwise dealt with inside the compromised account. A similar difficulty arises in other breach cases where it is not possible to identify with certainty exactly which records a threat actor viewed or accessed.[13] In those cases, as here, the

---

[12] I note that the definition of "use" contains a similar caveat: "'use', in relation to personal health information in the custody or under the control of a health information custodian or person, means … but does not include to disclose the information[.]"

[13] See for example PHIPA Decision 210, which I discuss further below.

determination of whether there has been a use of personal health information is made based on the available evidence.

[46] In this case, I consider the prevalence of personal health information in the email account, the fact the threat actor had unimpeded access to that information for a considerable period of time, and the threat actor's obvious intention to gain access to valuable information in SMDHU's email systems—which, in the case of a public health unit like SMDHU, clearly includes records of personal health information. In these circumstances, I am satisfied, on a balance of probabilities, that the threat actor used personal health information in the compromised email account during the window of opportunity available to it.

[47] There is no claim that this use occurred with the appropriate consent, or was permitted or required to be done without consent under *PHIPA*. In these circumstances, the use was not authorized by *PHIPA*. As a result, SMDHU is required to notify affected individuals of the unauthorized use.

[48] This interpretation is in keeping with the purposes of the duty to notify in section 12(2). Where an unauthorized third party had unimpeded access to a significant amount of personal health information for a considerable amount of time, it is reasonable to conclude, on a balance of probabilities, that there has been an unauthorized viewing, handling, or dealing with personal health information, and to require the custodian to notify the individuals to whom that information belongs. Notification serves the purpose of informing those individuals about the probable unauthorized activity involving information that, in a fundamental sense, belongs to them. Notified individuals may decide to seek more information from the custodian about the incident; complain to the IPC; seek a remedy; or take other steps they deem appropriate in the circumstances to mitigate the risks of the probable unauthorized activity involving their personal health information (e.g., heightened vigilance, credit monitoring).

[49] In summary, I have found that the threat actor's phishing attack on SMDHU's email systems resulted in both an unauthorized disclosure (by SMDHU to the threat actor) and an unauthorized use (by the threat actor) of personal health information in SMDHU's custody or control.

Implications of my findings of unauthorized disclosure and unauthorized use of personal health information

[50] My findings of unauthorized disclosure and unauthorized use of personal health information do not necessarily lead to a conclusion that SMDHU failed in its duty under *PHIPA* to take reasonable steps to protect the personal health information in its custody or control [section 12(1)]. The IPC has long recognized that the duty in section 12(1) of *PHIPA* to take "reasonable" steps does not call for perfection, and that there is no detailed

prescription in *PHIPA* for what is reasonable.[14] Moreover, in the context of similar obligations on institutions under *FIPPA* and *MFIPPA*,[15] the IPC has explicitly recognized that a breach may occur even where an institution had in place reasonable measures in compliance with its statutory obligations.[16] The requirement to take reasonable steps to protect personal health information does not call for a guarantee against cyberattacks or other threats of unauthorized disclosure or unauthorized use of personal health information.

[51] During the early resolution stage of the IPC process, SMDHU provided detailed information about its efforts to investigate and contain the phishing attack, and about its cybersecurity practices more generally. The IPC was satisfied with those aspects of SMDHU's response to the attack, and its compliance with its safeguarding obligations in section 12(1) of *PHIPA* is not at issue in this review.

[52] I have, however, found that the duty in section 12(2) to notify affected individuals applies. SMDHU was thus obligated to notify "at the first reasonable opportunity" all individuals whose personal health information was disclosed or used without authority as a result of the phishing attack. Under the next heading, I will consider whether SMDHU has met this duty in the circumstances.

B. If the duty to notify applies, was notice given in compliance with section 12(2)?

[53] Section 12(2) requires that the notice of theft, loss, or unauthorized use or disclosure of an individual's personal health information be given to that individual "at the first reasonable opportunity" [paragraph (a)], and that it include a statement of the individual's right to complain to the IPC [paragraph (b)].

[54] *PHIPA* does not specify the form of the notice required to be given under section 12(2).

[55] The IPC has observed that the appropriate form of notice may vary depending on the circumstances. In PHIPA Decision 110, for example, the IPC considered the relationship between the individuals affected by a privacy breach and the various custodians involved, the nature of the breaches, the publicity already given to the breaches, and the passage of time. In that case, the IPC found that the notification requirement could be met by means other than individual notices to affected individuals. The IPC found a more flexible approach to notification to be appropriate in the

---

[14] Among others, see PHIPA Decisions 44, 74, 82, and 124.
[15] Section 4(1) of General, RRO 1990, Reg 460 under *FIPPA*, and section 3(1) of General, RRO 1990, Reg 823 under *MFIPPA* contain identical wording, and read as follows: "Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected."
[16] IPC Privacy Complaint Report PR16-40, followed in Privacy Complaint Reports MC17-52 and MC18-17, among others.

circumstances, via notes in the files of affected patients, and notices posted in the private practice offices of some physicians.

[56] Similarly, in PHIPA Decision 210, involving a cyberattack against a hospital, the IPC considered a number of factors in determining the appropriate form of notice, including the very large number of potentially affected individuals, and the difficulty of determining with certainty exactly which individuals, and what information, had been affected by the attack. In that decision, the IPC found reasonable the hospital's decision to notify potentially affected individuals by posting a general notice on its website and issuing a news release publicizing the incident. These notices included all relevant details about the breach, including the nature of the cyberattack, the types of information that may have been affected by the cyberattack, the hospital's efforts to address the cyberattack, and the right to complain to the IPC.

[57] During the review, I invited SMDHU's representations on the matter of the appropriate form of notice to affected individuals in the event I find the duty to notify applies in this case. In doing so I noted the potential relevance of PHIPA Decision 210, concerning a cyberattack with some similar features to those present here.

[58] Despite its position that the duty to notify in section 12(2) does not apply, SMDHU decided during the IPC review to notify affected individuals of the cyberattack. SMDHU provided this notice in the form of letters to all individuals whose personal health information was contained in the compromised email account during a one-week period very close in time preceding the phishing attack. These letters included details about: the nature and extent of the breach; the specific personal health information affected by the breach; the steps taken by SMDHU to respond to the breach, including its report to the IPC; the contact information of an SMDHU agent who could respond to questions about the breach; and the individual's right to complain to the IPC, along with contact information for filing a complaint.

[59] Section 12(2) of *PHIPA* requires that notice of a breach be given "at the first reasonable opportunity." The phishing attack was discovered in July 2022. SMDHU did not send its letter notices to affected individuals until July 2023. This means that while SMDHU ultimately provided the notification required by section 12(2), the notice was given long after the first reasonable opportunity. However, in view of the notice that has been given, and the overall circumstances of the file, I conclude the review without issuing any order.

NO ORDER:

For the foregoing reasons, I find that the July 2022 email phishing attack on SMDHU email systems resulted in an unauthorized disclosure and an unauthorized use of personal health information within the meaning of section 12(2) of *PHIPA*.

Given the direct notice SMDHU provided to affected individuals during the IPC review, I find that SMDHU has provided the notification required by section 12(2), although it should have done so at the first reasonable opportunity. I conclude the review without issuing any order.

Original signed by: July 5, 2024

Jenny Ryu
Adjudicator