Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 253

File HR22-00498

The Hospital for Sick Children

July 5, 2024

Summary: In December 2022, the respondent the Hospital for Sick Children (the hospital) was the subject of a ransomware attack. The attack resulted in the encryption of numerous hospital servers, including those containing personal health information. However, the hospital's investigation did not find evidence of any access to or exfiltration of personal health information by the threat actor, or of any impact to the hospital's primary medical records system.

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 the hospital to notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or used or disclosed without authority. The hospital asserts that because the threat actor encrypted virtual servers at the "container" level, it did not "directly interact" with personal health information housed in the encrypted servers. The hospital takes the position that the attack did not result in a theft, loss, or unauthorized use or disclosure of personal health information within the meaning of section 12(2), and that the duty to notify does not apply.

In this decision, the adjudicator finds that the threat actor's encryption of hospital servers at the container level affected the personal health information in those servers, by making that information unavailable and inaccessible to authorized users. The ransomware attack resulted in both an unauthorized use and a loss of personal health information within the meaning of section 12(2). As a result, the hospital had a duty under *PHIPA* to notify affected individuals "at the first reasonable opportunity" of the incident. In the immediate aftermath of the attack, and in the weeks following, the hospital posted updates on its website and on social media informing the public about the attack, and of the progress of its investigation and remediation efforts. While the hospital's notice did not comply with section 12(2) because it did not include a statement

about the right to complain to the IPC, the adjudicator finds no useful purpose in directing that notice of the right to complain be given now. 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, 153, 175, 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 a ransomware encryption attack on the Hospital for Sick Children (the hospital), a health information custodian within the meaning of *PHIPA*.[2] For the reasons that follow, I find that an unauthorized third party's encryption of hospital servers containing personal health information resulted in the unauthorized use and loss of that information within the meaning of section 12(2) of *PHIPA*. As a result, the hospital had a duty to notify affected individuals at the first reasonable opportunity. In the immediate aftermath of the attack, and in the weeks following, the hospital posted updates on its website and on social media, informing the public about the nature and extent of the attack, and of the progress of its investigation and remediation efforts.

[1] PHIPA Decisions 254 and 255, and CYFSA Decision 19.
[2] Specifically, "the person who operates" the hospital is a health information custodian under paragraph 4.i of section 3(1) of *PHIPA*.

While these notices did not comply with the requirement in section 12(2) to include a statement about the right to complain to the IPC, in the circumstances I find no useful purpose in directing that further notice be given now. I conclude the review without making an order.

BACKGROUND:

[4] On December 18, 2022, the hospital discovered that it had been the victim of a ransomware attack after hospital staff began to experience network outages and difficulties accessing its virtual environment. The hospital immediately implemented its response protocols by retaining external legal counsel, which in turn engaged third-party cybersecurity experts to assist in containing and investigating the attack. The hospital also reported the incident to law enforcement.

[5] The hospital's forensic investigation determined that an unauthorized third party (the threat actor) had gained access to the hospital's environment through an employee's compromised credentials and had encrypted numerous hospital servers, the majority of which contained some form of personal health information. The investigation found no evidence that any personal health information was accessed or exfiltrated by the threat actor. It also determined that the hospital's primary medical records system was not accessed or otherwise affected by the attack.

[6] Based on this information, the hospital reported the incident to the Office of the Information and Privacy Commissioner of Ontario (IPC), but took the position that the ransomware encryption event did not result in any theft, loss, or unauthorized use or disclosure of personal health information, so that the duty in section 12(2) of *PHIPA* to the notify affected individuals did not apply. The IPC opened the present file to address this matter. The ransomware attack was the subject of wide media reporting, and despite its position that the duty to notify did not apply, the hospital provided regular public updates (including on its website and via social media) about the attack and the progress of its remediation efforts.

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

[8] However, this matter proceeded to adjudication to address outstanding issues arising from the hospital's position that the ransomware attack did not give rise to the duty 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.

[9] During the review, I sought and received representations from the hospital on whether the ransomware encryption event 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.[3]

[10] The hospital has asked that I withhold details of the hospital's cyber infrastructure, security measures, and cyber response capabilities, based on a concern that sharing these details publicly could put the hospital 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 the hospital's cybersecurity infrastructure and safeguards.[4]

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:

[11] 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.[5]

[12] As a preliminary matter, the hospital agrees that: 1) it is a health information custodian; 2) its information systems affected by the cyberattack contained personal health information; and 3) this personal health information was in the hospital's custody or control, within the meaning of those terms in *PHIPA*. There is no dispute that *PHIPA*

---

[3] I also asked the hospital 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 the hospital 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. I agree with the hospital that those orders are not relevant here, and I have not relied on them in making my determinations in this decision.

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

[5] 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.

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?

[13] 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.

[14] 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.

[15] 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.

[16] Despite its public communications about the ransomware attack, the hospital took the position that the duty to notify in section 12(2) of *PHIPA* does not apply, based on its view that the threat actor's encryption of select hospital servers at the container level did not involve any direct interaction with personal health information inside the encrypted servers. Thus, the hospital says, there was no theft, loss, or unauthorized use or disclosure of personal health information triggering the duty to notify.

[17] Even accepting that the ransomware encryption event at issue occurred only at the container level (and not at the individual file level), I conclude that the threat actor's

encryption of hospital servers containing personal health information resulted in both an unauthorized use and a loss of that information within the meaning of section 12(2). My reasons follow.

The ransomware encryption event resulted in the unauthorized "use" of personal health information within the meaning of section 12(2)

[18] 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),[6] but does not include to disclose the information, and "use", as a noun, has a corresponding meaning.

[19] 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.

[20] 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.

[21] The hospital asserts that the ransomware attack did not result in any unauthorized disclosure or use of personal health information. I will briefly address its arguments on disclosure before turning to my findings on use.

Disclosure

[22] The hospital notes that its forensic investigation found no evidence of data exfiltration by the threat actor.[7] In my Notice of Review to the hospital, I observed that

---

[6] 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).

[7] The hospital explained that to arrive at this conclusion, its forensic investigation team reviewed forensic artifacts related to software program execution and file and folder access activity, web browsing history,

this may support a finding that the ransomware attack did not result in any *further* disclosure of personal health information by the threat actor (for example, to the dark web or to any other person).

[23] However, it was my preliminary view that the threat actor's access to (infiltration of) the hospital's information systems, by itself, qualifies as a "disclosure" by the hospital to the threat actor of personal health information contained in the affected information systems, whether or not the hospital intended to disclose that information or was even aware of the threat actor's actions. In this context I noted the potential relevance of some IPC decisions that considered situations involving covert and unauthorized accesses by third parties to a custodian's information systems. 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 the unauthorized third party, despite the custodian's lack of intention to share that information with the unauthorized party.[8]

[24] The hospital argues that those situations are distinguishable from the facts at hand, because in those cases the personal health information was made available to the unauthorized parties "through a degree of recklessness on the part of custodians," and because "the custodians did something (whether intentionally or inadvertently)." By contrast, the hospital says, there is no evidence here of any error by the hospital that made personal health information available to the threat actor.

[25] In addition, the hospital says, the IPC decisions finding an unauthorized disclosure in the absence of a custodian's intention to disclose were made based on clear evidence that the unauthorized parties had accessed or viewed the personal health information at issue. By contrast, the hospital says, the ransomware encryption event at issue here occurred at the container level, and there is no evidence that individual files of personal health information housed in those containers were accessed, viewed, "interacted with," or exfiltrated by the threat actor. I understand the hospital's claim to be that no personal health information was actually "made available" to the threat actor when it infiltrated the hospital's information systems. I also understand this claim to relate to the hospital's technical arguments about the nature of the encryption event that occurred here.

[26] Because of my findings below, it is unnecessary to make a finding on whether the threat actor's infiltration of the hospital's information systems, on its own, qualifies as a "disclosure" of personal health information within the meaning of *PHIPA*, and I decline to

---

and network traffic logs. A different cybersecurity firm engaged by the hospital validated the findings of the forensic team and provided additional forensic analysis.

[8] Among them, PHIPA Decisions 49 and 110. 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.

do so. I note that I accept the hospital's evidence that there has been no exfiltration—and thus, no further disclosure by the threat actor—of personal health information that was contained in the information systems affected by the ransomware attack.[9]

Use

[27] I now turn to the issue of whether the ransomware attack resulted in the unauthorized "use" of personal health information in the hospital's information systems.

[28] The hospital maintains that the threat actor's encryption of its information systems containing personal health information was not a use of that information within the meaning of *PHIPA*.

[29] In PHIPA Decision 175, the IPC found that the term "use" in *PHIPA* includes the act or process of de-identifying personal health information. In my Notice of Review to the hospital, I shared a preliminary view that the act of encryption (in the context of a ransomware attack) is similar to the act of de-identification, in that both involve the modification, conversion, or other dealing with personal health information for purposes that can include concealment or obfuscation.

[30] The hospital submits that the reference to PHIPA Decision 175 is misplaced. First, the hospital notes that *PHIPA* defines "de-identification" as the "remov[al] [of] any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual."[10] The hospital states that there is no evidence in this case that encryption resulted in any de-identification of personal health information.

[31] The hospital next asserts that, in any event, the de-identification of information is not analogous to encryption. The hospital defines encryption, as it pertains to ransomware, as "the process by which data is encoded or scrambled, rendering it unreadable and inaccessible" and that "converts data into a form that cannot be read without the conversion method (a 'decryption key')."[11] The hospital says that the purpose of encryption in a ransomware attack is not to conceal the identity of any individual; instead, it says, the objective of ransomware encryption is typically to render an organization's systems unusable and provide a decryptor in exchange for a ransom payment.

[32] The hospital explains the difference between de-identification and encryption by way of an analogy to documents locked inside a file cabinet: While a threat actor may

---

[9] In PHIPA Decision 255, also released on this date, I reject a respondent's proposal to limit the meaning of "disclose" in *PHIPA* to positive and intentional actions by the disclosing party (and thus to exclude unintentional actions, as well as inaction, from the definition of disclose).

[10] At section 2 of *PHIPA*.

[11] The hospital cites the report of the cybersecurity firm it hired to validate the findings of the forensic investigation firm, and from the definition of "encryption" compiled by Trend Micro (a cybersecurity company), found online here: https://www.trendmicro.com/vinfo/us/security/definition.

change the lock on the cabinet (i.e., encryption), this does not, by itself, alter or conceal the cabinet's contents (i.e., de-identification) in the process. The hospital says that de-identification would in fact be counterproductive in the context of ransomware encryption, as the threat actor is reliant on the promise of harm to individuals by claiming to possess their information (i.e., information that has not been de-identified). In the hospital's submission, it therefore follows that the threat actor's encryption of the hospital's network did not "use" personal health information within the meaning of *PHIPA*.

[33] I accept the hospital's definition of ransomware encryption as a process by which data is encoded or scrambled, making it unreadable and inaccessible to those without the decryption key. I accept the hospital's assertion that the purposes of de-identification and encryption are different, and in fact may be incompatible with one another in the context of a ransomware encryption event.

[34] However, it does not follow from these differences in end purposes that the definition of use cannot apply to both de-identification and ransomware encryption. I remain of the view that the acts of using personal health information for de-identification and for encryption are analogous in that both acts involve a kind of handling of or dealing with personal health information.

[35] The hospital's more significant argument against a finding of use is based on a technical description of the type of ransomware encryption attack that occurred in this case. This argument concerns the difference between encryption at the "container" level, and encryption at the file level.

[36] The hospital explains that there are two distinct modes of carrying out ransomware attacks by way of encryption. Threat actors can deploy ransomware (malware) directly onto specific files that are stored on computers and servers, resulting in the encryption of those specific files. Alternatively, threat actors can deploy ransomware at the "container" level, by encrypting virtualized servers rather than the data stored within those servers. (Virtualized servers operate as containers that store operating systems and user files.)

[37] The hospital explains that by encrypting the container, threat actors can affect the availability of the information stored inside the container without ever needing to open, view, or interact with the files inside the container. In addition, once the container is encrypted, the threat actor itself cannot access or view the contents without decrypting the container. The hospital provides the following analogy to explain the difference between the two approaches: Encrypting specific files stored on a system is like walking through every room of a building and locking individual doors, while encrypting at the container level is like locking the doors to the entire building, without having to access the individual rooms inside.

[38] The hospital explains that the threat actor in this case employed the second method (container-level encryption), by deploying ransomware on the hospital's

underlying virtualization server. The hospital says that by encrypting the containers that house the operating system and user files, the threat actor was able to encrypt many systems at once without having to "directly interact" with those operating systems and user files. In the hospital's submission, this means no personal health information was viewed or encrypted, and thus no personal health information was "used" within the meaning of *PHIPA*.

[39] I accept the hospital's evidence that the threat actor's encryption of hospital servers occurred at the container level, rather than at the level of individual files of personal health information housed within those severs. For the purposes of this decision, I am also prepared to accept the hospital's evidence that the threat actor did not view or access any individual files of personal health information housed within the hospital's environment that the threat actor infiltrated. However, the question remains whether the personal health information in the affected servers was "handled" or "otherwise dealt with," and thus "used" within the meaning of *PHIPA*. I find that the personal health information was used in this way.

[40] This is because I do not accept the hospital's assertion that the threat actor's locking (by encryption) of external containers housing personal health information has no effect on that information. Instead, it is my view that the transformation (by encryption) of external containers also transforms the personal health information housed within those containers—at a minimum, by making that personal health information unavailable and inaccessible to authorized users of that information. The effect of making unavailable to the hospital the personal health information held within the encrypted containers is, I find, a kind of "handling" of or "dealing with" that information, and thus a use within the meaning of *PHIPA*.

[41] The hospital argues that to the extent any personal health information was inaccessible during the ransomware attack, backups of that information were readily available. But the restoration of personal health information from backups does not negate the fact that something happened to the personal health information inside the encrypted containers, giving rise to the need to restore that information. The availability of backups to restore the affected personal health information does not preclude a finding of use.

[42] I also note that this use of personal health information occurs whether or not the threat actor actually views or accesses specific files of personal health information held within the affected containers, or exfiltrates that information outside the hospital's environment. It is my finding that the act of encrypting containers housing personal health information is, by itself, a use of that information within the meaning of *PHIPA*.

[43] 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 threat actor's encryption of hospital servers was an unauthorized use of personal health information within the meaning of section 12(2).

[44] The result of this finding is that the hospital had a duty to notify affected individuals of the unauthorized use of their personal health information. This outcome is consistent with the purpose of notification, which is to inform individuals of unauthorized activities involving information that, in a fundamental sense, belongs to them. Notified individuals may decide to seek more information from the custodian about the breach and risks associated with the breach; complain to the IPC; seek a remedy; or take other steps they deem appropriate in the circumstances to mitigate the risks in response to the breach (e.g., heightened vigilance, credit monitoring).

[45] As I have found the ransomware attack resulted in an unauthorized use of personal health information, the duty to notify in section 12(2) applies, and the hospital was obligated to notify "at the first reasonable opportunity" all individuals whose personal health information was affected by the attack.

The ransomware encryption event resulted in the "loss" of personal health information within the meaning of section 12(2)

[46] The duty to notify in section 12(2) also arises in the event personal health information in the custody or control of a custodian is stolen or lost.[12] There is no definition of "lost" or "loss" in *PHIPA*.

[47] The hospital submits that a finding of loss in this case would not be supported by the case law and would not reflect the mechanics of the encryption that occurred. The hospital says that previous IPC decisions that found a loss of personal health information involved situations where that information was destroyed or misplaced—where the losses were crystallized and, to a degree, permanent.[13] By contrast, the hospital says, the ransomware attack at issue here did not result in a permanent lack of access to the affected servers or to the personal health information contained in them, since backups of the servers were not affected by the attack and were available to support the hospital's clinical functions.[14] In these circumstances, the hospital says, there was no "loss" of personal health information.

[48] A robust backup policy is an important component of an organization's information security practices.[15] In this case, the hospital had in place policies and practices that

---

[12] Some ransomware attacks could also result in the theft of personal health information. Given my findings in this decision, it is unnecessary for me to consider whether the ransomware encryption attack at issue in this review also resulted in the theft of personal health information.

[13] The hospital cites an IPC report in File HI-050042-1 (A Hospital Emergency Department), in which copies of emergency department records were inadvertently shredded; and PHIPA Decision 70, in which a social worker misplaced two physical files containing personal and medical information.

[14] In the aftermath of the ransomware attack, the hospital publicly reported that despite the threat actor's offer of a free decryptor, it did not use the decryptor to restore systems and did not make a ransom payment.

[15] Maintaining regular backups of information and systems in an offline environment is one of the measures the IPC recommends in its Technology Fact Sheet "How to Protect Against Ransomware" (updated October 2022). Available online: https://www.ipc.on.ca/.

enabled it to quickly restore its information systems and resume its clinical functions. The hospital's information practices were key to its ability to quickly recover from the cyberattack.

[49] However, the restoration of affected systems from backups does not negate the fact that, for some period of time, personal health information in the custody or control of the hospital was made inaccessible to it as a result of the threat actor's attack on its information systems. Specifically, the ransomware encryption attack had the effect of denying authorized users (i.e., the hospital) access to personal health information that it required to provide services. As the hospital publicly reported, the consequences of this loss of availability included delays retrieving lab and imaging results, and some resulting diagnostic and treatment delays.

[50] The distinction drawn by the hospital between encryption occurring at the file level and encryption occurring at the container level makes no practical difference to my finding. In either case, the effect on an individual's personal health information is the same: that information is made unavailable to the authorized user of that information because of an unauthorized activity. I find this is a "loss" of that information within the meaning of section 12(2) of *PHIPA*, and the duty to notify is thus also triggered for this reason.

[51] In defining loss in this way, I distinguish this situation from other routine or non-routine disruptions in a custodian's ability to access or otherwise use personal health information in its custody or control for authorized purposes. For example, a scheduled software or hardware maintenance operation or an unexpected power outage may also disrupt, for a temporary period, a custodian's ability to access personal health information in its custody or control for authorized purposes. An overly broad interpretation of the terms "lost" and "loss" in section 12(2) could require the notification of individuals in situations like these, which would not in my view serve the purpose of the duty to notify. Further, it is not difficult to imagine how an overly broad interpretation of loss could lead to notification fatigue on the part of the public, disproportionate costs to the custodian, and other unintended and undesirable consequences.

[52] Instead, I adopt a purposive definition of these terms in section 12(2) that, in the context of a ransomware attack, contemplates notice to affected individuals where there has been an unauthorized action in respect of their personal health information. It is consistent with the purposes of section 12(2) that individuals be notified of a third party's malicious action done with the intention of, and having the effect of, denying a custodian access to those individuals' personal health information in the custodian's custody or control.

[53] The purpose of the duty to notify in these circumstances is to inform individuals about the unauthorized action involving information that, in a fundamental sense, belongs to them. These individuals should be made aware if the custodian is not able to access their personal health information as a result of unauthorized activity, and of the risks

associated with that activity. It is also consistent with a purposive reading of this section not to require notification in a situation like routine maintenance or a power outage, which may disrupt a custodian's ability to access personal health information, but which is not the result of unauthorized activity and is not likely to increase the risk of unauthorized activity. The latter situations generally would not qualify as a loss under section 12(2).[16] The different outcomes in these different scenarios are in keeping with the purposes of the duty to notify in *PHIPA*.

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

[54] My findings of unauthorized use and loss of personal health information do not necessarily lead to a conclusion that the hospital 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.[17] Moreover, in the context of similar obligations on institutions under *FIPPA* and *MFIPPA*,[18] 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.[19] The requirement to take reasonable steps to protect personal health information does not call for a guarantee against cyberattacks or other threats of unauthorized use or loss of personal health information.

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

[56] However, having found that the ransomware attack resulted in both an unauthorized use and a loss of personal health information, the duty in section 12(2) to notify affected individuals applies. Under the next heading, I will consider whether the hospital has met this duty in the circumstances.

---

[16] Assuming, of course, that the custodian is able to regain access to personal health information after these events are complete.
[17] Among others, see PHIPA Decisions 44, 74, 82, and 124.
[18] 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."
[19] IPC Privacy Complaint Report PR16-40, followed in Privacy Complaint Reports MC17-52 and MC18-17, among others.

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

[57] 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)].

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

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

[60] 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.

[61] During the review, I invited the hospital's representations on the appropriate form of notice to affected individuals in the event I find the duty to notify applies in this case.

[62] The hospital asks that if I find the duty to notify applies, I consider the hospital's response to the breach in deciding whether to order notification. The hospital submits that its remedial actions in the aftermath of the breach were prompt, appropriate, and reasonable. The hospital refers to an IPC decision in which the IPC found no purpose in directing a custodian to give notice of certain privacy breaches in view of the particular circumstances of that case, including the passage of time since the breaches and the relatively benign circumstances surrounding the breaches.[20] The hospital also cites a number of other cases in which the IPC and other regulators ordered that notice be given,

[20] The hospital cites PHIPA Decision 153, in which the custodian determined that a nurse mistakenly accessed patient records when failing to comply with a new internal hospital process.

which the hospital says demonstrate that such orders are appropriate where there has been exfiltration of sensitive data.[21] The hospital notes, again, that there is no evidence of exfiltration in this case.

[63] I am not persuaded that an order for notice is appropriate only where there has been exfiltration of personal health information. The language of section 12(2) makes clear that the duty to notify arises in the event personal health information in the custody or control of a custodian is stolen or lost, or is used or disclosed without authority. However, the decisions cited above illustrate that the IPC applies a contextual and flexible approach to determining the appropriate form of notice, taking into account relevant circumstances that may include the nature and volume of the personal health information at issue, the remedial actions of the custodian, and the passage of time.

[64] In this case, the hospital took prompt steps to investigate and to contain the cyberattack, including by engaging third-party forensic experts, notifying law enforcement, and fully cooperating with the IPC in this review. In the immediate aftermath of the attack, and for several weeks afterward, the hospital posted regular updates on its website and on social media, informing the public about the nature and extent of the incident and of the progress of the hospital's investigation and remediation efforts. These regular communications kept the public apprised of the effects of the ransomware attack, including on the hospital's clinical functions, and the timelines for the restoration of its systems. Additionally, there was widespread media coverage of the ransomware attack and the hospital's responses.

[65] While the hospital's communications served the purpose of informing the public about the attack, they failed to notify affected individuals about the right to complain to the IPC, as required by section 12(2)(b) of *PHIPA*. However, through this IPC-initiated file, the IPC has considered issues under *PHIPA* arising from the ransomware attack, including the sufficiency of the hospital's responses and its notification obligations. Considering the overall circumstances, including the passage of time, I find there is no useful purpose in directing that further notice be given now. I therefore conclude this review without making an order.

NO ORDER:

For the foregoing reasons, I find that the December 2022 ransomware attack on hospital servers containing personal health information resulted in an unauthorized use and a loss

[21] Among others, the hospital cites PHIPA Decision 210 (in which a threat actor accessed a hospital's network and exfiltrated "a very large amount of personal health information"); *Newfoundland and Labrador (Health and Community Services) (Re)*, 2023 CanLII 43735 (NL IPC) (concerning a 2021 cyberattack on the province's healthcare systems that resulted in the exfiltration of over 200 gigabytes of data); and *eHealth Saskatchewan, Saskatchewan Health Authority, Ministry of Health (Re)*, 2021 CanLII 214 (SK IPC) (concerning a ransomware attack that resulted in the theft of approximately 40 gigabytes of encrypted data from the province's health authorities).

of personal health information within the meaning of section 12(2) of *PHIPA*. As a result, the hospital had a duty to notify affected individuals at the first reasonable opportunity of the breach.

While the hospital's notice of the breach did not comply with section 12(2) because it did not include a statement about the right to complain to the IPC, in the circumstances I find no useful purpose in directing that notice of the right to complain be given now. I conclude the review without issuing any order.

Original signed by: July 5, 2024

Jenny Ryu
Adjudicator