Information and Privacy Commissioner,
Ontario, Canada

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

# CYFSA DECISION 19

File FR22-00009

Halton Children's Aid Society

July 5, 2024

**Summary:** In February 2022, the respondent Halton Children's Aid Society (CAS) was the subject of a ransomware attack. While the CAS's investigation did not find any evidence that the threat actor had accessed or exfiltrated any data stored in the CAS's environment, it found that the threat actor had encrypted several CAS servers, including those containing personal information.

The IPC initiated a review of the matter under Part X of the *Child, Youth and Family Services Act, 2017* (*CYFSA*). Section 308(2) of the *CYFSA* sets out a duty on service providers like the CAS to notify individuals at the first reasonable opportunity if their personal information is stolen, lost, or used or disclosed without authority. The CAS asserts that because the ransomware attack targeted its servers at the external or "container" level, the attack did not "individually impact" file folders and files of personal information held inside the encrypted containers. The CAS takes the position that the encryption event did not result in a theft, loss, or unauthorized use or disclosure of personal information within the meaning of section 308(2), and that the duty to notify does not apply.

In this decision, the adjudicator finds that the threat actor's encryption of CAS servers at the container level affected the personal information in those servers, by making that personal information unavailable and inaccessible to authorized users. The ransomware attack resulted in both an unauthorized use and a loss of personal information within the meaning of section 308(2). As a result, the CAS had a duty to notify affected individuals "at the first reasonable opportunity" of the incident. After taking into account relevant circumstances, including the evidence of diligent efforts by the CAS to contain and to mitigate the risks of the privacy breach, the adjudicator finds that the notice requirement can be met in this case through the posting of a general notice on the CAS's website, or another form of indirect public notice. The adjudicator orders the CAS to provide this notice within 30 days of the date of this decision.

**Statutes Considered:** *Child, Youth and Family Services Act, 2017*, SO 2017, c 14, Sch 1, sections 2 (definitions), 286, 291(1)(a) and (g), 308(1) and (2), and 318(1); Personal Information, O Reg 191/18 under the *Child, Youth and Family Services Act, 2017*, section 8; *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Sch A, sections 2 (definitions), 12(1) and (2), and 37(1) and (2); 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, 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 Part X of the *Child, Youth and Family Services Act, 2017* (*CYFSA*) and the *Personal Health Information Protection Act, 2004* (*PHIPA*). These statutes require covered organizations to take reasonable steps to protect the security of individuals' personal information (or personal health information under *PHIPA*) 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 information or personal health 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 attack on the Halton Children's Aid Society (CAS), a service provider under the *CYFSA*.[2] For the reasons that follow, I find that an unauthorized third party's encryption of CAS servers containing personal information resulted in the unauthorized use and loss of that information within the meaning of section 308(2) of the *CYFSA*. As a result, the CAS had a duty to notify affected individuals at the first reasonable opportunity. I order the CAS to provide this notice, and in the circumstances find that indirect public notice (for example, through a posting on the CAS's website) will satisfy the notice requirement.

---

[1] PHIPA Decisions 253, 254, and 255.

[2] "Service provider" is defined in section 2(1) of *CYFSA*, and incorporates other terms ("society," "service") that are further defined in sections 2(1), 34(1), and 281.

## BACKGROUND:

[4] On February 22, 2022, the CAS discovered that it had been the victim of a cyberattack when its backup software program alerted it to the premature termination of a scheduled backup process. While the CAS's internal IT team immediately disconnected its servers, interrupting the unauthorized third party's (the threat actor's) encryption process, the attack nonetheless resulted in the full encryption of some CAS systems.

[5] The CAS retained external breach counsel, which in turn engaged an external forensic firm to conduct a forensic investigation into the cyberattack, and a third party to negotiate with the threat actor. The forensic investigation firm determined that the threat actor's encryption of select servers "did not result in any access to or exfiltration of data," including personal information, in the CAS's servers.

[6] Based on this information, the CAS 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 information, so that the duty in section 308(2) of the *CYFSA* to notify affected individuals did not apply. The IPC opened the present file to address this matter.

[7] At the early resolution stage of the IPC process, IPC staff sought and received updates from the CAS about the ransomware attack, including about the nature and scope of the attack, the actions taken by the CAS to investigate and to remediate its systems after the attack, and the CAS's cybersecurity practices more broadly. The CAS worked cooperatively with the IPC to provide this information. By the end of the early resolution stage, IPC staff were satisfied with the CAS's investigation and containment efforts. Those aspects of the CAS'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 CAS'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 318(1) of the *CYFSA*. Section 318(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 Part X of the *CYFSA* or its regulations.

[9] During the review, I sought and received representations from the CAS on whether the ransomware encryption event resulted in the theft, loss, or unauthorized use or disclosure of personal information, within the meaning of those terms in section 308(2) of the *CYFSA*, and, if so, the appropriate form of notice in the circumstances.[3]

[3] I also asked the CAS to comment on the potential relevance to my review of IPC Orders HO-004 and HO-007, which were issued under *PHIPA*. 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

[10] The CAS has asked that I withhold details of its security safeguards, based on a concern that sharing these details publicly could put the CAS (and potentially other service providers) at an increased risk of future cybersecurity attacks. I accept this request, and in this decision I have wherever possible left out references to the specifics of the CAS's security safeguards.[4]

## ISSUES:

A. Does the notification requirement in section 308(2) of the *CYFSA* apply in the circumstances?

B. If notice is required under section 308(2), what form of notice is appropriate in the circumstances?

## DISCUSSION:

[11] Among other purposes, Part X of the *CYFSA* sets out rules to ensure the security of "personal information" that has been collected for the purpose of providing a "service" and that is in the "custody" or "control" of a service provider.[5]

[12] As a preliminary matter, the CAS agrees that: 1) it is a service provider; 2) its information systems affected by the cyberattack contained personal information that was collected for the purpose of providing a service; and 3) this personal information was in the CAS's custody or control, within the meaning of those terms in the *CYFSA*. There is no dispute that Part X of the *CYFSA* applies to the personal information at issue in this review.

### A. Does the notification requirement in section 308(2) of the *CYFSA* apply in the circumstances?

[13] Section 308 of the *CYFSA* sets out obligations on service providers to take reasonable steps to protect the security of personal information in their custody or

---

information accessed outside normal network protections. While the CAS 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 CAS 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 information" is defined in section 2 of the *CYFSA* to have the same meaning as in *FIPPA*. As noted above, "service" and "service provider" are defined terms in the *CYFSA* (sections 2(1), 281).

"Custody" and "control" are not defined in the *CYFSA*. However, the IPC has interpreted these terms in the *CYFSA* 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 *PHIPA*: CYFSA Decision 4 and PHIPA Decision 232, among others.

control. Section 308(1) states:

> A service provider shall take reasonable steps to ensure that personal information that has been collected for the purpose of providing a service and that is in the service provider'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 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 information is affected by a privacy breach, in accordance with section 308(2). This section states:

> Subject to any prescribed exceptions and additional requirements, if personal information that has been collected for the purpose of providing a service and that is in a service provider's custody or control is stolen or lost or if it is used or disclosed without authority, the service provider shall,
>
> (a) notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or 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 section 316.

[16] In this case, the CAS decided not to notify individuals based on its position that the threat actor's encryption of select CAS servers at the outer or container levels did not have an impact on individual file folders or files of personal information housed within those servers. Thus, the CAS says, there was no theft, loss, or unauthorized use or disclosure of personal 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 CAS servers containing personal information resulted in both an unauthorized use and a loss of that information within the meaning of section 308(2). My reasons follow.

### *The ransomware encryption event resulted in the unauthorized "use" of personal information within the meaning of section 308(2)*

[18] Section 286 of the *CYFSA* sets out rules for the collection, use, and disclosure of personal information collected by a service provider for the purpose of providing a service

to an individual. Under this section, the *CYFSA* authorizes the "use" and "disclosure" of personal information in some circumstances—namely, where there is the appropriate consent (and other conditions are met); or where the *CYFSA* permits or requires the use or disclosure to be made without consent.

[19] If a use or disclosure occurs outside these circumstances, then that use or disclosure is not authorized under the *CYFSA*. In such a case, the personal information will have been "used or disclosed without authority" within the meaning of section 308(2), and the duty to notify will be triggered.

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

*Disclosure*

[21] "Disclosure" is not a defined term in the *CYFSA*. However, in its guidance to service providers governed by Part X of the *CYFSA*, the IPC has said that generally, disclosure means releasing information or making the information available to another person or organization.[6]

[22] The CAS relies on the findings of the external forensic firm that it retained to investigate the cyberattack. The forensic investigation did not find any evidence that the threat actor exfiltrated (i.e., removed from the CAS's environment) any personal information stored in CAS systems.[7] The CAS also notes that the threat actor denies having exfiltrated any data from the CAS's environment.[8] Based on these circumstances, the CAS concludes there was no disclosure of personal information.

[23] In my Notice of Review to the CAS, I shared a preliminary view that the threat actor's access to (infiltration of) the CAS's information systems containing personal information qualifies as a "disclosure" of personal information by the CAS to the threat actor, whether or not the CAS 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 issued under *PHIPA* 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

---

[6] IPC, "Part X of the Child, Youth and Family Services Act: A Guide to Access and Privacy for Service Providers" (May 2019), at pages 13 and 16. Available online: https://www.ipc.on.ca/.

[7] The CAS provided details of how the forensic investigation team reached this conclusion. Among other things, the forensic team analyzed available logs and artifacts to determine the threat actor's activities within the CAS's information systems, and monitored the threat actor's known leak site for evidence of any personal information or other data belonging to the CAS.

[8] The CAS explains that in the case of a ransomware attack, it would be in the threat actor's best interest to provide proof of any exfiltration.

share that information with the unauthorized party.[9]

[24] The CAS argues that the cyberattack on its information systems does not qualify as a "disclosure" within the meaning of the *CYFSA* because (unlike in the *PHIPA* examples described above) this attack did not result in any actual access by the threat actor to personal information contained in the affected systems. I understand the CAS's claim to be that no personal information was actually "made available" to the threat actor when it infiltrated the CAS's information systems and encrypted certain CAS servers. I also understand this claim to relate to the CAS's technical arguments about the nature of the ransomware encryption event that occurred here.

[25] Because of my findings below, it is unnecessary to make a finding on whether the threat actor's infiltration of the CAS's information systems, on its own, qualifies as a "disclosure" of personal information within the meaning of the *CYFSA*, and I decline to do so. I note that I accept the CAS's evidence that there has been no further disclosure by the threat actor, to the dark web or to any other person, of personal information that was contained in the information systems affected by the ransomware attack.

*Use*

[26] I now turn to the issue of whether the ransomware attack resulted in the unauthorized "use" of personal information in the CAS's information systems. The *CYFSA* does not contain a definition of the term. However, in its guidance to service providers, the IPC has said that generally, using personal information means viewing or dealing with the information in a manner that does not include disclosing it.[10]

[27] The CAS maintains that the threat actor's encryption of its information systems is not a use of personal information within the meaning of the *CYFSA*.

[28] First, the CAS submits that the term "use" should not be applied to actors other than service providers as defined by the *CYFSA*. The CAS says that section 2(1) states that the purpose of the service provider is to offer services under the *CYFSA*, and does not contemplate unauthorized actors.[11] The CAS then directs my attention to paragraph (a) of section 291(1), which sets out a permitted use of personal information. Section 291(1)(a) states:

> A service provider may use personal information collected for the purpose of providing a service […] for the purpose for which the information was collected or created and for all the functions reasonably necessary for

[9] Among them, PHIPA Decisions 49 and 110. I discuss these decisions in more detail further below.
[10] See footnote 6, above.
[11] The term "service provider" is defined at section 2(1) of the *CYFSA* to cover several enumerated parties, including, at paragraph (c) of the definition, "a person or entity, including a society, that provides a service funded under [*CYFSA*] […] but does not include a foster parent."

> carrying out that purpose, including providing the information to an officer, employee, consultant or agent of the service provider […]

[29] The CAS states that the modern approach to statutory interpretation requires that unless ambiguous, the provisions of a statute are to be interpreted in accordance with their plain reading and legislative purpose.[12] In the CAS's submission, applying the modern approach leads to a reading of sections 2(1) and 291(1)(a) that limits the categories of persons who may "use" personal information to those persons who fall under the statutory definition of service provider (as well as any officers, employees, consultants, and agents who receive information necessary to carry out services as permitted by the service provider). The CAS thus asserts that the term "use" in the *CYFSA* cannot apply to third parties such as threat actors.

[30] I do not agree with the CAS's proposed limitation on the meaning of use in the *CYFSA*.

[31] To begin, I see no support for this interpretation in the sections of the *CYFSA* cited by the CAS. Section 291(1)(a) of the *CYFSA*, to which the CAS directed my particular attention, and section 291(1) more broadly, set out specified circumstances in which service providers governed by the *CYFSA* may use personal information that was collected for the purpose of providing a service. The fact that these sections of the *CYFSA* limit these discretionary powers to service providers is consistent with the purpose of these sections, which is to establish narrow and specific circumstances in which service providers may use individuals' personal information without their consent. The fact these specific use permissions apply only to service providers (and not to third parties like threat actors) is not, in my view, indicative of a legislative intention to limit the application of all other use-related provisions to service providers.

[32] More generally, I find the CAS's proposed interpretation to be inconsistent with the text as well as the purposes of sections 308(1) and (2) of the *CYFSA*. These sections address the duties on a service provider to protect "personal information that has been collected for the purpose of providing a service" and that is in the "service provider's custody or control," including against unauthorized use. These sections do not explicitly limit these protections to situations where the unauthorized use is committed by an "insider" (i.e., the service provider, or an officer, employee, consultant, or agent of the service provider), and I see no interpretive principle that justifies reading in such a limitation here.

[33] Under the CAS's proposed interpretation, the rules and protections in Part X of the *CYFSA* concerning the use of personal information would apply only to the actions of service providers (and those acting on their behalf), and not to the actions of third parties (such as threat actors). Such an interpretation could frustrate one of the very purposes

---

[12] The CAS cites *Rizzo & Rizzo Shoes Ltd (Re)*, [1998] 1 SCR 27 at para 21.

of Part X of the *CYFSA*, which is to protect personal information.

[34] Consider a situation where a party, without authorization, inserts and executes a malicious code in a service provider's information system that alters the contents of personal information within the system (with or without removing that information from the system). Where the malicious action is committed by an insider, the duty to notify affected individuals about the unauthorized use of their personal information would apply. But under the CAS's proposed interpretation, the same action committed by a third party would not be an unauthorized use of personal information, and may not otherwise trigger the duty to notify individuals whose personal information is altered by the third party's malicious action.

[35] I find unreasonable an interpretation of "use" that makes the duty to notify contingent on whether the person who views or otherwise deals with personal information in an unauthorized manner is internal or external to the organization. Such an interpretation would be inconsistent 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 service provider 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). I am not persuaded that the importance of notifying individuals is in any way diminished when it is an unauthorized third party, rather than a service provider (or an officer, etc., of the service provider), who uses their personal information without authorization. In fact, I find it reasonable to expect that the privacy risks to individuals could be heightened—and the need for notification more urgent—in the case of an unauthorized third party actor.

[36] Besides this, I observe that no such limitation applies to the term "use" in *PHIPA*. While not identical to Part X of the *CYFSA*, *PHIPA* is a statute that is also administered by the IPC, and that sets out very similar rules to protect the privacy of individuals with respect to their personal information (personal health information in *PHIPA*), among other purposes. I note that *PHIPA* contains analogous sections to those in the *CYFSA* on which the CAS relied in support of its statutory interpretation argument, as described above.[13]

[37] The term "use" is defined in *PHIPA* as follows:

---

[13] Specifically, like the *CYFSA*, *PHIPA* identifies certain persons (called health information custodians in *PHIPA*) who are subject to its rules concerning the collection, use, and disclosure of individuals' personal information (personal health information in *PHIPA*): section 3 of *PHIPA* and section 3 of General, O Reg 329/04. Also like Part X of the *CYFSA*, *PHIPA* sets out certain permitted uses of that information, including one that is analogous to the use specified in section 291(1)(a) of the *CYFSA*: section 37(1)(a) of *PHIPA*. And like the *CYFSA*, *PHIPA* limits these specific use permissions to certain persons: sections 37(1) and (2) of *PHIPA*.

> "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), but does not include to disclose the information, and "use", as a noun, has a corresponding meaning[.][14]

[38] This definition in *PHIPA* does not limit the "use" of personal health information to particular actors. Applying the definition in *PHIPA*, the IPC has found in many cases that third parties acting without the authority of a health information custodian "used" personal health information (in contravention of *PHIPA*), including in situations where the custodian had no knowledge of the third parties' actions.[15] Moreover, in PHIPA Decision 49, the IPC found that a third party who was neither a custodian nor an agent of the custodian "used" personal health information in the custody or control of the custodian (and did so without authorization).[16]

[39] In its guidance to service providers about the meaning of the term "use" in the *CYFSA*, the IPC has drawn from the definition of the identical term in *PHIPA*. The IPC has said that generally, using personal information means viewing or dealing with the information in a manner that does not include disclosing it.[17] I agree with this definition of "use" for the purposes of the *CYFSA*, which I find to be consistent with the ordinary meaning of the term, and I adopt it here.

[40] The identical term in *PHIPA* does not explicitly contain, and has not been interpreted to contain, the limitation proposed by the CAS. More importantly, and as I have explained above, such a limitation on the meaning of "use" would be inconsistent with a purposive interpretation of the duty to notify in the *CYFSA*.

[41] For all these reasons, I conclude that the term "use" in section 308 of the *CYFSA* can apply to the activities of third parties, and not only to the activities of those persons who are identified in the statutory definition of service provider in section 2(1).[18]

[42] Next, the CAS objects to a preliminary view, which I had shared in my Notice of

---

[14] At section 2(1) of *PHIPA*. Section 6(1), which is referred to in the definition of "use," specifies that the providing of personal health information between a custodian and an agent of the custodian is a "use" of that information (and not a disclosure by the custodian and corresponding collection by the agent).

[15] PHIPA Decisions 62, 110, and 168, among others, involve agents of custodians acting in specified instances without the authority of the custodian—for example, by viewing records of personal health information of friends, family, and colleagues without having a health care purpose or other authorized purpose for the use.

[16] PHIPA Decision 49 involved a patient who was left unsupervised in a doctor's office and took photographs of a computer screen displaying the personal health information of other patients. See also PHIPA Decision 205, which involved an email phishing attack on an agent's email account. There was no dispute in that case that the phishing attack resulted in the unauthorized use of personal health information in the custodian's custody or control.

[17] See footnote 6, above.

[18] And any officers, employees, consultants, or agents of the service provider contemplated by section 291(1)(a).

Review, that the act of encrypting personal information qualifies as a "use" of that information for the purposes of the *CYFSA*. I explained that in forming this preliminary view, I found relevant section 291(1)(g) of the *CYFSA*, which identifies as a "use" in the *CYFSA* an activity carried out for the purpose of disposing of or modifying personal information to conceal the identity of an individual. In response, the CAS makes both general and specific arguments against such a finding.

[43] The general argument has to do with the purposes of encryption more broadly. The CAS takes issue with an analogy I had proposed in the Notice of Review to the circumstances in PHIPA Decision 175, in which the IPC found that the act or process of de-identifying personal health information is a "use" of that information within the meaning of *PHIPA*. The CAS notes that *PHIPA* contains a definition of "de-identify," which reads as follows:

> "de-identify", in relation to the personal health information of an individual, means to remove 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, and "de-identification" has a corresponding meaning[.][19]

[44] The CAS states that the purpose and method of encryption in a ransomware event is different than the purpose of de-identification. It says that the purpose of encryption is not to conceal the identity of an individual, but rather to render an organization's systems unusable, and provide a decryptor in exchange for a ransom payment. The CAS says that in an encryption event, de-identification would in fact be counterproductive to a threat actor's motive, since the threat actor is reliant on the promise of harm to individuals by claiming to possess their personal information (i.e., not de-identified information). Therefore, the CAS says, the encryption of its network did not "conceal" (and thus did not "use") any personal information within the meaning of section 308(2) of the *CYFSA*.

[45] I accept the CAS's definition of 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')." Ransomware is "a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid."[20] I accept the CAS'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.

[46] However, it does not follow from these differences in end purposes that the

---

[19] At section 2 of *PHIPA*.

[20] The CAS cites (but does not appear to directly quote from) the definitions of "encryption" and "ransomware" compiled by Trend Micro (a cybersecurity company), found online here: https://www.trendmicro.com/vinfo/us/security/definition.

definition of use cannot apply to both de-identification and ransomware encryption. I remain of the view that the acts of using personal information for de-identification and for encryption are analogous in that both acts involve a kind of dealing with personal information.

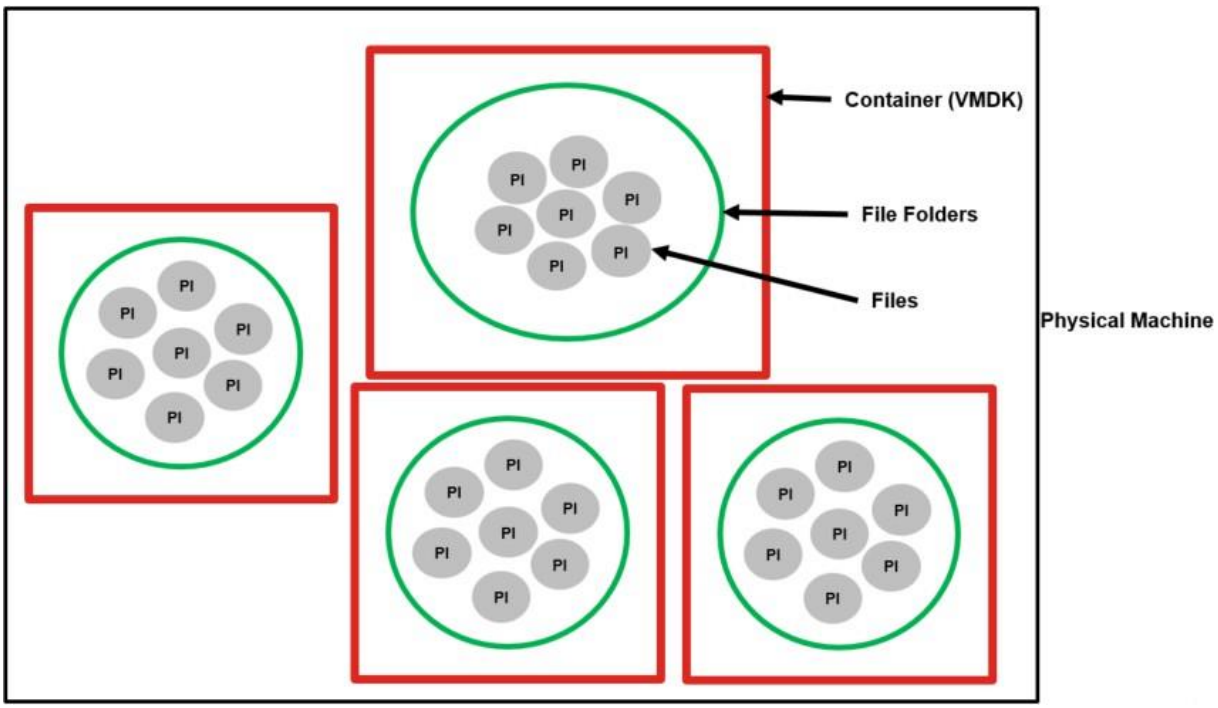
[47] I will next consider the CAS's more significant arguments about why the specific encryption event that occurred in this case did not result in a use of personal information. This argument is based on a technical description of how this particular attack works.

[48] The CAS provided detailed explanations of how ransomware encryption functions, including on the development and exchange of encryption keys and the relationship between ransomware operators and affiliates. In this case, the CAS says, the threat actor encrypted the CAS's virtual machines ("VMs") at the container level (the "VMDK file"), and not at the individual file level. A VM uses software instead of a physical system to run programs, and several VMs can be run on one physical machine.

[49] The CAS acknowledges that the threat actor's locking (by encryption) of its VMs made any files or data held within the VMs inaccessible to those without the decryption key. However, the CAS says, this encryption process affected "only the outer 'container' levels." It is the CAS's assertion that encryption occurring at the container level has no impact on any individual file folders and files of personal information held within the encrypted containers. I find helpful in understanding this argument an analogy the CAS made to a threat actor who locks a file cabinet containing documents. In this analogy, the threat actor may have changed the lock on the cabinet (i.e., performed container-level encryption) but in doing so does not alter the contents of the cabinet.[21]

[50] The CAS provided the following diagram to illustrate its point. It says that while the external container (red) has been locked by encryption, the internal file folders (green) and files containing personal information (grey) "are not individually impacted. An encryption event simply 'locks' the outermost layer of the host."

[21] The CAS offered this analogy in the context of its arguments for drawing a distinction between encryption and de-identification. Specifically, the CAS proposed that encryption is like the act of locking the cabinet, while de-identification is like the act of redacting each file held within the cabinet.
I find the file cabinet analogy equally helpful to understanding the CAS's argument that encryption at the container level does not necessarily entail a threat actor's access to (i.e., use of) any individual files of personal information housed within the encrypted container.




[51] The CAS reports that its forensic investigation team found no evidence that the threat actor opened, viewed, staged, or exfiltrated data in the CAS's environment, or that it accessed any folders housing personal information. The CAS's conclusion is that the cyberattack that occurred here was a "encryption-only event" that did not involve any access to or exfiltration of personal information, and thus did not result in any use of personal information within the meaning of the *CYFSA*.

[52] I accept the CAS's evidence that the threat actor's encryption of the CAS's information systems occurred at the VM or container level, and not at the level of individual file folders or files housed within the affected VMs. For the purposes of this decision, I am also prepared to accept the CAS's evidence that the threat actor did not open, view, or otherwise access any individual files of personal information housed within the CAS environment that the threat actor infiltrated. However, the question remains whether the personal information housed within the affected VMs was otherwise "dealt with," and thus "used" within the meaning of the definition I have set out above. I find that the personal information was used in this way.

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

[54] This use of personal information occurs whether or not the threat actor actually opens or views specific files of personal information held within the affected containers, or exfiltrates that information outside the service provider's environment. It is my finding that the act of encrypting containers housing personal information is, by itself, a use of that information within the meaning of the *CYFSA*.

[55] There is no claim that this use occurred with the appropriate consent, or was permitted or required to be done without consent under section 291 of the *CYFSA*. In these circumstances, I conclude that the threat actor's encryption of CAS servers was an unauthorized use of personal information within the meaning of section 308(2).

[56] As I have found the ransomware attack resulted in an unauthorized use of personal information, the duty to notify in section 308(2) applies, and the CAS is obligated to notify "at the first reasonable opportunity" all individuals whose personal information was affected by the attack.

### *The ransomware encryption event resulted in the "loss" of personal information within the meaning of section 308(2)*

[57] The duty to notify in section 308(2) also arises in the event "personal information that has been collected for the purpose of providing a service and that is in a service provider's custody or control is stolen or lost."[22] There is no definition of "lost" or "loss" in the *CYFSA*.

[58] As noted above, the CAS defines ransomware encryption as "the process by which data is encoded or scrambled, rendering it unreadable and inaccessible," and ransomware as "a type of malware that prevents or limits users from accessing their system […] until a ransom is paid." The CAS concedes that any files or data within VMs encrypted by the threat actor "would have been inaccessible after encryption," and that the purpose of encryption in a ransomware event is "to render an organization's systems unusable."

[59] The CAS notes that because of the robust backup policy it had in place prior to the cyberattack, it was able to restore its systems and information immediately following the containment of its IT environment.[23] The CAS refers to detailed information it provided to the IPC about its data replication and backup process. The CAS also states that most of its work is carried out through the Child Protection Information Network (CPIN), a provincial information system used by children's aid societies to store information needed to deliver child protection services in the province, and that its access to CPIN was not affected by the cyberattack. The CAS thus asserts that through backups and access to

[22] Some ransomware attacks could also result in the theft of personal 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 information.

[23] The CAS acknowledges that the cyberattack prevented it from using certain internal systems for one week following discovery of the attack; however, the CAS says, all functionality and access to the affected networks and file servers was restored from backups.

CPIN, it had all the information it needed to continue its work as a service provider. On this basis, it is the CAS's view that no personal information was "lost" to it as a result of the attack.

[60] A robust backup policy is an important component of an organization's information security practices.[24] In this case, the CAS had in place policies and practices that enabled it to quickly restore its information systems and resume its statutory duties as a service provider under the *CYFSA*. The CAS's information practices were key to its ability to quickly recover from the cyberattack.

[61] However, the restoration of affected systems from backups does not negate the fact that, for some period of time, personal information in the custody or control of the CAS was made inaccessible to the CAS as a result of the threat actor's attack on the CAS's information systems. Specifically, the ransomware encryption attack had the effect of denying authorized users (i.e., the CAS) access to personal information that they required for the purpose of providing services. Here I note that the distinction drawn by the CAS 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 information is the same: the personal 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 308(2) of the *CYFSA*, and the duty to notify is thus also triggered for this reason.

[62] In defining loss in this way, I distinguish this situation from other routine or non-routine disruptions in a service provider's ability to access or otherwise use personal 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 service provider's ability to access personal information in its custody or control for authorized purposes. An overly broad interpretation of the terms "lost" and "loss" in section 308(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 service provider, and other unintended and undesirable consequences.

[63] Instead, I adopt a purposive definition of these terms in section 308(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 information. It is consistent with the purposes of section 308(2) that individuals be notified of a third party's malicious action done with the intention of, and having the effect of, denying a service provider access to those individuals' personal information collected for the purpose of providing a

[24] 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/.

service and in the service provider's custody or control.

[64] The purpose of the duty to notify in these circumstances is to inform individuals about the unauthorized action involving personal information that, in a fundamental sense, belongs to them. These individuals should be made aware if the service provider is not able to access their personal 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 service provider's ability to access personal 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 308(2).[25] The different outcomes in these different scenarios are in keeping with the purposes of the duty to notify in the *CYFSA*.

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

[65] My findings of unauthorized use and loss of personal information do not necessarily lead to a conclusion that the CAS failed in its duty under the *CYFSA* to take reasonable steps to protect the personal information in its custody or control [section 308(1)]. The IPC has long recognized, in the context of the equivalent duty on health information custodians in *PHIPA*,[26] that the statutory duty to take "reasonable" steps does not call for perfection, and that there is no detailed prescription in the statute for what is reasonable.[27] Moreover, in the context of similar obligations on institutions under *FIPPA* and *MFIPPA*,[28] 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.[29] The requirement to take reasonable steps to protect personal information does not call for a guarantee against cyberattacks or other threats of unauthorized use or loss of personal information.

[66] During the early resolution stage of the IPC process, the CAS 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

---

[25] Assuming, of course, that the service provider is able to regain access to personal information after these events are complete.

[26] Section 12(1) of *PHIPA*, which reads: "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."

[27] Among others, see PHIPA Decisions 44, 74, 82, and 124.

[28] 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."

[29] IPC Privacy Complaint Report PR16-40, followed in Privacy Complaint Reports MC17-52 and MC18-17, among others.

CAS's response to the attack, and its compliance with its safeguarding obligations under section 308(1) of the *CYFSA* is not at issue in this review.

[67] However, having found that the ransomware attack resulted in both an unauthorized use and a loss of personal information, the duty in section 308(2) to notify affected individuals applies. Under the next heading, I will consider how the CAS can meet this duty in the circumstances.

**B. If notice is required under section 308(2), what form of notice is appropriate in the circumstances?**

[68] I reproduce section 308(2) for ease of reference:

> Subject to any prescribed exceptions and additional requirements, if personal information that has been collected for the purpose of providing a service and that is in a service provider's custody or control is stolen or lost or if it is used or disclosed without authority, the service provider shall,
>
> (a) notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or 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 section 316.

[69] Regulations to the *CYFSA* provide additional detail about the contents of the notice to be given under section 308(2). Specifically, section 8 of Regulation 191/18 under the *CYFSA* (Personal Information) states:

> The following additional requirements are prescribed for the purposes of subsection 308 (2) of the Act:
>
> 1. The service provider shall notify the individual in plain, easy-to-understand language, and the notification shall include a general description of how the personal information was lost, stolen or used or disclosed without authority.
>
> 2. The service provider shall inform the individual of any steps the service provider has taken to,
>
> i. prevent a similar theft or loss or unauthorized use or disclosure of personal information from recurring, and
>
> ii. mitigate possible adverse effects on the individual that may be caused by the theft or loss or unauthorized use or disclosure.

> 3. The service provider shall provide the individual with the contact information of an employee of the service provider who can provide the individual with additional information about the theft or loss or unauthorized use or disclosure.

[70] The *CYFSA* does not specify the form of notice required to be given under section 308(2).

[71] In considering the analogous duty to notify in *PHIPA*,[30] 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.

[72] 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.

[73] Although the IPC made these findings under *PHIPA*, I find the contextual and flexible approach to notification endorsed in those decisions to be an appropriate model for considering the analogous requirement in the *CYFSA*. I adopt the same approach here.

[74] Section 308(2) requires the CAS to notify affected individuals of the breach "at the first reasonable opportunity." As the cyberattack was discovered in February 2022, the "first reasonable opportunity" has long since passed. The CAS has a duty to provide this

---

[30] Section 12(2) of *PHIPA*, which states: "Subject to subsection (4) [which concerns notice in the event personal health information that was disclosed to a researcher is subject to a privacy breach] 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."

notification without undue delay.

[75] Considering relevant factors including the passage of time and the evidence of diligent efforts by the CAS to contain and to remediate the effects of the cyberattack, I am satisfied that a flexible approach to notification is appropriate in the circumstances. I will thus not require the CAS to provide direct notice to affected individuals. Instead, the CAS can fulfil its notice obligations under section 308(2) through means such as posting a notice on its website or issuing a public release. Whatever method of indirect notice it chooses, the CAS must ensure that the notice complies with the requirements of section 308(2) and section 8 of Regulation 191/18 under the *CYFSA*.

## ORDER:

For the foregoing reasons, I find that the February 2022 cyberattack on the CAS's servers containing personal information collected for the purpose of providing a service and in the CAS's custody or control resulted in an unauthorized use and a loss of personal information within the meaning of section 308(2) of the *CYFSA.*

Pursuant to section 321(1)(c), I order the CAS to comply with the duty to notify in section 308(2) and section 8 of Regulation 191/18. In doing so, the CAS should have regard to the guidance provided at paragraph 75 of this decision. The CAS is to provide this notice within **30 days** of the date of this decision.

Original signed by: July 5, 2024

Jenny Ryu
Adjudicator