CITATION: Hospital for Sick Children v. Ontario (Information and Privacy Commissioner), 2025 ONSC 5208
DIVISIONAL COURT FILE NO.: 449/24, 450/24 & 453/24
DATE: 20250916

ONTARIO

SUPERIOR COURT OF JUSTICE
DIVISIONAL COURT

Sachs, Lococo and A.D. Kurke JJ.

BETWEEN:	
THE HOSPITAL FOR SICK CHILDREN Applicant	*Christine Muir* and *Travis Walker*, for the Applicant
– **and** –	
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO Respondent	*Brendan Gray*, for the Respondent
– **and** –	
ONTARIO HOSPITAL ASSOCIATION Intervenor	*Daniel Girlando* and *Hanna Rioseco*, for the Intervenor
AND BETWEEN:	
HALTON CHILDREN'S AID SOCIETY Applicant/Appellant	*Christine Muir* and *Travis Walker*, for the Applicant/Appellant
– **and** –	
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO Respondent	*Brendan Gray*, for the Respondent
	HEARD at Toronto: May 1, 2025

REASONS FOR JUDGMENT

R. A. LOCOCO J.

I. Introduction

[1] The Hospital for Sick Children ("SickKids") seeks judicial review of the decision of the respondent Information and Privacy Commissioner of Ontario (the "IPC" or the "Commissioner") dated July 5, 2024, reported at 2024 CanLII 67095 (ON IPC) (the "SickKids Decision").

[2] Halton Children's Aid Society ("Halton" or "CAS", and together with SickKids, the "Applicants") appeals and seeks judicial review of the IPC's decision dated July 5, 2024, reported at 2024 CanLII 67087 (ON IPC) (the "Halton Decision", and together with the SickKids Decision, the "Decisions").

[3] At issue before the IPC was alleged non-compliance with Ontario privacy legislation. Under that legislation, the Applicants are required to notify individuals, at the first reasonable opportunity, of the theft, loss, or unauthorized use of their personal information that is in the Applicants' possession or control. The notification is required to include a statement about the individuals' entitlement to make a complaint to the IPC about the privacy breach.

[4] Following separate cybersecurity incidents (known as "ransomware" attacks), the Applicants were temporarily unable to access individuals' personal information on the Applicants' servers. After investigation, the Applicants concluded that the perpetrators were not able to view, access or exfiltrate any of the data. Both Applicants notified the IPC of the ransomware attacks but took the position that the requirement to notify affected individuals had not been engaged. SickKids (but not Halton) publicly disclosed the attack, without referring to the entitlement to complain to the IPC.

[5] In the Decisions, the IPC found that privacy breaches had occurred, and that the Applicants had failed to comply with the requirement to notify affected individuals. In the Halton Decision, the IPC ordered Halton to provide the required notice by posting a notice on its website or issuing a public release. In the SickKids Decision, the IPC did not issue a remedial order. The adjudicator found no useful purpose in doing so, given SickKids previous public disclosure.

[6] The Applicants submit that the IPC erred and was unreasonable in determining that there was an unauthorized "use" or a "loss" of personal information that required notification. The Ontario Hospital Association (the "OHA") intervened to support their position. The Applicants ask that the Decisions be set aside.

[7] The IPC submits that it was correct and reasonable to find that the Applicants were required to notify affected individuals about the ransomware attacks. The IPC also argues that SickKids's application should be dismissed on grounds of mootness in the absence of a remedial order.

[8] While I would not dismiss SickKids's application as moot, I would dismiss the judicial review applications and the appeal on the merits.

II. Background

A. The parties

[9] SickKids is a pediatric hospital located in Toronto. It is a "health information custodian" as defined in the *Personal Health Information Protection Act, 2004*, S.O. 2004 c. 3, Sched. A ("*PHIPA"*) and an "institution" as defined in s. 2(1) of the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31 ("*FIPPA*"). Because of those designations, SickKids has certain rights and obligations respecting the collection, use and disclosure of "personal information" and "personal health information" for its purposes: see *PHIPA*, s. 3(1). (In these reasons, "personal information" as defined in s. 2(1) of *FIPPA* and "personal health information" as defined in s. 4 of *PHIPA* are sometimes referred to collectively as "personal information".)

[10] Halton is a designated children's aid society pursuant to s. 34(1) of the *Child, Youth and Family Services Act, 2017*, S.O. 2017, c. 14, Sched. 1 (the "*CYFSA*"). Its services include (i) the investigation of allegations that children may be in need of protection, (ii) protection of children where necessary, (iii) providing guidance, counselling and other services to families respecting the protection of children, (iv) providing care or supervision for children assigned to its care or supervision, and (v) placing children for adoption: see *CYFSA*, s. 35(1). Pursuant to Part X (Personal Information) of the *CYFSA*, Halton is a "service provider" that collects and maintains in its custody and control "personal information" for the purpose of providing its services: see *CYFSA*, ss. 281-332. For this purpose, the term "personal information" has the same meaning as in *FIPPA*: see *CYFSA*, s. 2(1). (In these reasons, a "service provider" as defined is s. 281 of the CYFSA and a "health information custodian" as defined in s. 2 of *PHIPA* are sometimes referred to collectively as an "information custodian".)

[11] The IPC provides oversight of Ontario's access to information and privacy laws, including as set out in *PHIPA* and Part X of the *CYFSA*. The IPC is appointed pursuant to s. 4(2) of *FIPPA*. The IPC has authority to initiate and conduct reviews of potential contraventions of *PHIPA*, Part X of the *CYFSA* and the regulations under those statutes: see *PHIPA*, s. 58(1); *CYFSA*, s. 318(1).

B. Notification requirements

i. PHIPA "health information custodian"

[12] As part of its obligations under *PHIPA* as a "health information custodian", SickKids is required to safeguard the personal health information in its custody or control and, in certain circumstances, to notify affected individuals and the IPC if the security of that information is compromised. Section 12 of *PHIPA* provides in part:

> **Security**
> **12**(1) 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.

Notice of theft, loss, etc. to individual
(2) Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,

(a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and

(b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

Notice to Commissioner
(3) If the circumstances surrounding a theft, loss or unauthorized use or disclosure referred to in subsection (2) meet the prescribed requirements, the health information custodian shall notify the Commissioner of the theft or loss or of the unauthorized use or disclosure.

[Emphasis added.]

[13] The term "use" is defined in *PHIPA* but "lost" (or "loss") is not. In s. 2 of *PHIPA*, "use" is defined as follows:

> "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. ("utiliser", "utilisation") [Emphasis added.]

[14] The entitlement to make a complaint to the Commissioner under Part VI (Complaints, Reviews and Inspections) of *PHIPA* is set out in s. 56(1), which provides:

Complaint to Commissioner
56(1) A person who has reasonable grounds to believe that another person has contravened or is about to contravene a provision of this Act or its regulations may make a complaint to the Commissioner.

ii. CYFSA "service provider"

[15] As a "service provider" under the *CYFSA*, Halton has corresponding obligations relating to the "personal information" in its custody or control. Section 308 of the *CYFSA* provides:

Steps to ensure security of personal information
308(1) 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.

Notice of theft, loss, etc. to individual
(2) 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.

Notice to Commissioner and Minister
(3) If the circumstances surrounding the theft, loss or unauthorized use or disclosure meet the prescribed requirements, the service provider shall notify the Commissioner and the Minister of the theft, loss or unauthorized use or disclosure.

[Emphasis added.]

[16] The terms "use" and "lost" (or "loss") are not defined in the *CYFSA*.

[17] The entitlement to make a complaint to the Commissioner under Part X of the *CYFSA* is set out in s. 316(1), which provides:

Complaint to Commissioner
316(1) A person who has reasonable grounds to believe that another person has contravened or is about to contravene a provision of this Part or the regulations made for the purposes of this Part may make a complaint to the Commissioner.

C. The ransomware attacks

[18] In 2022, the information systems of Halton and SickKids were targeted by separate ransomware attacks. Ransomware is a type of malware that encrypts the victim's data, making it inaccessible until a ransom is paid.

[19] As the Applicants indicate, there are different ways attackers (or "threat actors") go about encrypting data. One is by encrypting individual data files identified on various computers or servers. Another is by encrypting operating system files which are stored in virtual disk images or "containers", which house individual files. If encryption occurs at the container level, the act of encryption does not itself indicate that the threat actor has accessed, viewed, or exfiltrated the data within the container. Rather, once the container is encrypted, neither the threat actor nor the health information custodian or service provider can access or view its contents until it is decrypted.

[20] On February 22, 2022, Halton became aware of a ransomware attack on its systems (the Halton "attack" or "ransomware attack"). On December 18, 2022, SickKids discovered the ransomware attack on its systems (the SickKids "attack" or "ransomware attack").

[21] Each Applicant advised the IPC of the ransomware attack affecting their systems within a few days of learning of it. However, as explained below, the Applicants say they provided notice to the IPC as a courtesy only, arguing that the statutory notification requirement was not engaged.

[22] Despite taking that position, SickKids (unlike Halton) provided public notice of the SickKids attack by announcement on its website and social media on December 19, 2022, the day after learning of the attack. SickKids provided further public updates on December 22, 23 and 29, 2022 and January 5, 2023, confirming their conclusion that there was no evidence of any impact on personal health information. SickKids's public disclosure did not refer to an individuals' entitlement to make a complaint to the IPC under s. 56 of *PHIPA*.

D. The IPC review

[23] After receiving notice from the Applicants, the IPC opened a file about the ransomware attacks and requested further information. Both Applicants had retained legal counsel and forensic/cybersecurity experts to assist in containment and investigation of the attacks. The Applicants and their counsel provided the IPC with updates of the progress of their investigations and other requested information.

[24] As a result of their investigations, the Applicants concluded that the encryption of their servers occurred at the container level. They advised the IPC that certain information was temporarily unavailable, but they were able to recover information from back-up systems and their day-to-day operations were largely unaffected. They also advised that their investigations found no evidence that any personal information had been viewed, opened, accessed, copied or exfiltrated.

[25] On March 7, 2023, the IPC issued a Notice of Review under s. 318(1) of the *CYFSA*, to determine whether the Halton attack gave rise to a notification obligation under s. 308(2) of the *CYFSA*. In its submissions and throughout the review, Halton argued that the Halton attack did not result in any unauthorized "use" or "disclosure", or (in supplementary submissions) any "loss" of personal information such that notice was required.

[26] On June 1, 2023, the IPC issued a Notice of Review under s. 58(1) of *PHIPA* relating to the SickKids attack to determine whether the container-level encryption of systems containing personal health information gave rise to a notification obligation under s. 12(2) of *PHIPA*. In its submissions and throughout the review, SickKids emphasized that the SickKids attack did not result in any theft, loss, or unauthorized "use" or "disclosure" of personal health information in its custody or control since no personal health information had been viewed, accessed, copied, exfiltrated, or otherwise interacted with by the threat actor.

[27] To explain the method of encryption and its lack of impact on any data files containing personal health information, SickKids drew an analogy to a filing cabinet, stating that container-level encryption is akin to changing the lock on the cabinet, which renders the files inside

inaccessible but otherwise intact and their contents unaffected. The IPC accepted this analogy in its decision: SickKids Decision, at para. 32.

E. The Decisions

[28] The IPC adjudicated and issued both the SickKids Decision and the Halton Decision on July 5, 2024. In each case, for substantially similar reasons, the IPC found that ransomware attack resulted in both an unauthorized "use" and a "loss" of personal information within the meaning of the applicable legislation. Therefore, the IPC concluded that the Applicants were required to notify affected individuals of the attacks "at the first reasonable opportunity": see *PHIPA*, s. 12(2); *CYFSA*, s. 308(2).

[29] On the same day as the Decisions, the IPC issued two other decisions that stemmed from cyberattacks on health information custodians subject to *PHIPA*: *Kingston, Frontenac and Lennox & Addington (KFL&A) Public Health (Re)*, 2024 CanLII 67096 (ON IPC); *Simcoe Muskoka District Health Unit (Re)*, 2024 CanLII 67094 (ON IPC). In each decision, the IPC found that cyberattack resulted in both an unauthorized "use" and a "loss" of personal information within the meaning of s. 12(2) of *PHIPA*. These decisions (like the Decisions being considered by this panel) each included the same statement under the heading "Overview" (in each case at para. 2):

> 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.

i. Unauthorized use of information

[30] In the SickKids Decision, at paras. 39-43, the IPC provided the following justification for its finding that the ransomware attack result in an unauthorized "use" of personal health information within the meaning of s. 12(2) 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).

[31] In the Halton Decision, at paras. 52-55, the IPC provided substantially similar reasoning for finding that the Halton ransomware attack resulted in an unauthorized use of personal information within the meaning of s. 308(2) of the *CYFSA*.

ii. Loss of information

[32] In the SickKids Decision, at paras. 47-53, the IPC provided the following justification for its finding that the ransomware attack result in the "loss" of the personal health information within the meaning of s. 12(2) of *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. 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. 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. In this case, the hospital had in place policies and

practices that 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). The different outcomes in these different scenarios are in keeping with the purposes of the duty to notify in *PHIPA*.
>
> [Footnotes omitted.]

[33] In the Halton Decision, at paras. 58-64, the IPC provided substantially similar reasoning for finding that the ransomware attack resulted in the loss of personal information within the meaning of s. 308(2) of the *CYFSA*.

iii. Remedy

[34] In the SickKids Decision, the IPC noted that SickKids made appropriate public disclosure of the SickKids attack in its aftermath. However, the IPC found that the notice did not comply with s. 12(2) of *PHIPA* because it did not include a statement about the right to complain to the IPC. The IPC also decided that there was no useful purpose in directing SickKids to provide notice of the right to complain at that time. Therefore, the IPC concluded its review without issuing a remedial order.

[35] In the Halton Decision, in the absence of prior public disclosure of the Halton attack, the IPC decided to make a remedial order as a result of Halton's noncompliance with the notification requirement in s. 308(2) of the *CYFSA*. As set out in the Summary of the Halton Decision, the IPC found:

> After taking into account relevant circumstances, including the evidence of diligent efforts by the [Halton] 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.

[36] In deciding the notice on Halton's website or other form of indirect notice was sufficient, the IPC considered and rejected requiring Halton to provide direct notice to individuals, stating that it was satisfied that a flexible approach to notification is appropriate in the circumstances: Halton Decision, at para. 75.

III. Judicial review applications and appeal

[37] By Notice of Application for Judicial Review dated August 6, 2024, SickKids seeks judicial review of the SickKids Decision.

[38] By Notice of Appeal and Notice of Application for Judicial Review both dated August 6, 2024, Halton appeals and seeks judicial review of the Halton Decision.

[39] On August 8, 2024, the IPC granted an interim stay of the Halton Decision. The stay was confirmed on a final basis on August 28, 2024, and remains in effect until resolution of Halton's application for judicial review and its appeal.

[40] By order dated November 4, 2025, Shore J. directed that the SickKids's judicial review application and Halton's judicial review application and appeal be heard together.

[41] By order dated March 27, 2025 (with reasons at 2025 ONSC 1911), Shore J. granted leave to the OHA to intervene as a friend of the court in the judicial review applications and the appeal.

A. Jurisdiction and standard of review

[42] The Divisional Court has jurisdiction to hear SickKids's judicial review application: see *Judicial Review Procedure Act*, R.S.O. 1990, c. J.1 (the "*JRPA*"), ss. 2, 6(1).

[43] The Divisional Court has jurisdiction to hear Halton's appeal, but only on a question of law: *CYFSA*, s. 322(1). Despite any right of appeal, the Divisional Court has jurisdiction to hear Halton's judicial review application: *JRPA*, ss. 2, 6(1). Judicial review is a discretionary and extraordinary remedy, but the existence of a right of appeal limited to questions of law does not in itself amount to a discretionary bar nor preclude a judicial review application for questions of fact or mixed fact and law: *Yatar v. TD Insurance Meloche Monnex*, 2024 SCC 8, 489 D.L.R. (4th) 191, at para. 57.

[44] On an appeal from an administrative decision, the appellate standards of review apply: *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65, [2019] 4 S.C.R. 653, at para. 37. The standard of review is correctness for questions of law: *Housen v. Nikolaisen*, 2002 SCC 33, [2002] 2 S.C.R. 235, at para. 8. For Halton's appeal, there is no appeal with respect to questions of fact or questions of mixed fact and law except where there is an extricable question of law, which is reviewable on a correctness standard: *Housen*, at paras. 26-37; *CYFSA*, s. 322(1).

[45] Upon judicial review, the presumptive standard of review is reasonableness: *Vavilov*, at paras. 23-25. For the Applicants' judicial review applications, there is no dispute that the standard of review is reasonableness.

[46] Reasonableness review "finds its starting point in the principle of judicial restraint" but remains "a robust form of review" rather than "a 'rubber-stamping' process or a means of sheltering administrative decision makers from accountability": *Vavilov*, at para. 13. A reasonable decision is one that is based on an internally coherent and rational chain of analysis that is justified in relation to the facts and law that constrain the decision maker. The reasonableness standard requires a reviewing court to defer to such a decision: *Vavilov*, at para. 85. The relative expertise of administrative decision makers with respect to the questions before them is a relevant consideration in conducting reasonableness review: *Vavilov*, at paras. 31, 92-93.

[47] The burden is on the party challenging the decision to show that it is unreasonable. Before a decision can be set aside on that basis, "the reviewing court must be satisfied that there are sufficiently serious shortcomings in the decision such that it cannot be said to exhibit the requisite degree of justification, intelligibility and transparency": *Vavilov*, at para. 100.

B. Issues for determination

[48] The Applicants submit that the IPC erred and was unreasonable in determining that there was an unauthorized "use" or a "loss" of personal information. In doing so, the Applicants say that the IPC improperly engaged in a results-oriented interpretive exercise, rather than considering the text, context and purpose of the statutory provisions, as required by the principles of statutory interpretation.

[49] The OHA supports the Applicants' position. The OHA submits that the IPC's interpretation of the notification requirements will lead to useless over-notification and an unnecessary burden on information custodians.

[50] The IPC submits that it was correct and reasonable in deciding that the Applicants were required to notify affected individuals about the ransomware attacks. The IPC also argues that SickKids's application should be dismissed on grounds of mootness in the absence of a remedial order.

[51] The issues for determination are as follows:

a. Mootness: Should SickKids's application be dismissed on grounds of mootness?

b. Approach to statutory interpretation: Did the IPC engage in improper results-oriented interpretation of the statutory provisions?

c. Unauthorized "use" of information: Have the Applicants established that the IPC erred and was unreasonable in finding that there was an unauthorized "use" of information?

d. Loss of information: Have the Applicants established that the IPC erred and was unreasonable in finding that there was a "loss" of information?

[52] Those issues are addressed below in turn.

IV. Analysis and conclusions

A. SickKids's application should not be dismissed on grounds of mootness

[53] As a preliminary matter, the IPC submits that SickKids's judicial review application should be dismissed on grounds of mootness.

[54] Given my conclusion (explained below) that both judicial review applications and Halton's appeal should be dismissed on the merits, it appears unnecessary to decide whether SickKids

application should also be dismissed on grounds of mootness. However, brief reasons are being provided to explain why it was appropriate to consider SickKids's application despite the absence of a remedial order.

[55] In *Borowski v Canada (Attorney General)*, [1989] 1 S.C.R. 342, at pp. 353-54, the Supreme Court confirmed that the doctrine of mootness applies "when the decision of the court will not have the effect of resolving some controversy which affects or may affect the rights of the parties. If the decision of the court will have no practical effect on such rights, the court will decline to decide the case."

[56] As a general principle, courts do not decide moot cases: *Borowski*, at pp. 353-54; *Maystar General Contractors Inc. v. International Union of Painters and Allied Trades, Local 1819*, 2008 ONCA 265, 90 O.R. (3d) 451, at para. 26. The onus falls to the party seeking to have the case decided to justify the court's departure from this principle by proceeding to hear and decide the matter: *Mayfair*, at para. 32; *Tamil Co-operative Homes Inc. v. Arulappah* (2000), 49 O.R. (3d) 566 (C.A.), at para. 17.

[57] At the first stage of the analysis, the court must determine whether the case is moot, which requires an assessment of whether a live controversy remains between the parties. If there is no live controversy, the case is moot: *Borowski*, at p. 354; *Mayfair*, at para. 27.

[58] If the case is found to be moot, the court moves to the second stage of the analysis – to assess whether to exercise discretion to hear a moot case: *Borowski*, at pp. 358-63; *Maystar*, at paras. 33-34. To make this determination, the court considers three factors (listed below), recognizing that "the ultimate determination is not a mechanical process" (*Maystar*, at para. 33):

a. The presence or absence of an appropriate adversarial context;

b. The concern for judicial economy; and

c. The need for the court to be sensitive to its role as the adjudicative branch in our political framework.

[59] In support of their position that SickKids's application should be dismissed on grounds of mootness, the IPC says that (i) there is no longer an adversarial relationship between the parties in relation to the SickKids Decision, (ii) the IPC's review of SickKids response to the ransomware attack is complete, and (iii) no remedial order was issued against SickKids. Among other things, the IPC submits that whatever decision this court makes on judicial review, it will have no practical impact on SickKids's legal obligation relating to the ransomware attack. The IPC also argues that despite any wider issues that may be raised in SickKids's judicial review application, the court is able to address those issues in its decision relating to the Halton Decision, which is being considered by the same panel.

[60] As explained below, I do not agree that SickKids's application should be dismissed on grounds of mootness.

[61] On the preliminary issue of whether the matter is moot, I conclude that a live controversy remains between SickKids and the IPC. Therefore, I do not consider the case to be moot.

[62] While the SickKids Decision did not include a remedial order, the IPC decided that SickKids's public notification did not comply with s. 12(2) of the *PHIPA*. SickKids challenges that conclusion and continues to argue that notification should not be required for the encryption-based cyber attack of the type at issue. It is clear that in the current proceedings, SickKids (with the OHA's support) and the IPC "have continued to argue their respective positions vigorously", supporting the conclusion that a live controversy remains: see *Mayfair*, at para. 34.

[63] But even if the matter is considered moot, I am satisfied that the court should exercise discretion to hear SickKids's judicial review application.

[64] Addressing the first factor in the analysis, there is no doubt that there is an "appropriate adversarial context" in this case, as discussed above: see *Mayfair*, at para. 34.

[65] With respect to judicial economy (the second factor in the analysis), judicial review of the SickKids Decision is being conducted in conjunction with a corresponding judicial review under a different statute that raises substantially the same issues (except mootness). Therefore, there is no significant additional strain on judicial economy as a result of SickKids's judicial review application.

[66] With respect to the court's adjudicative function (the third factor), to the extent that there is any doubt as to whether a notification requirement was triggered by the ransomware attack at issue, it is appropriate for the court to adjudicate the matter to assist in resolving outstanding issues of concern. The OHA's intervention indicates a broader public interest (beyond the parties) in the issues under consideration, which militates in favour of hearing the application. The wider interest is also indicated by the *KFL&A* and *Muskoka Simcoe* decisions the IPC issued the same day about alleged privacy breaches under *PHIPA* relating to individuals' personal health information that (the IPC found) "in a fundamental sense, belongs to" the affected individuals: SickKids Decision, at para. 53.

[67] Accordingly, I conclude that SickKids's judicial review application should not be dismissed on grounds of mootness.

B. The IPC did not engage in improper results-oriented analysis

[68] The Applicants argue that in interpreting the statutory notification requirements (including the terms "used" and "lost" in s. 12(2) of *PHIPA* and s. 308(2) of the *CYFSA*), the IPC improperly engaged in "results-oriented reasoning", in order to "reverse-engineer the desired outcome". The Applicants say that approach was inconsistent with the ordinary and fundamental terms of statutory interpretation.

[69] In *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27, at para. 21, the Supreme Court concisely stated the modern principle of statutory interpretation, previously formulated in Elmer A. Driedger, *Construction of Statutes*, 2nd ed. (Toronto: Butterworths, 1983), at p. 87:

> Today there is only one principle or approach, namely, the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.

[70] In *Blue Star Trailer Rentals Inc. v. 407 ETR Concession Company Limited*, 2008 ONCA 561, 91 O.R. (3d) 321, after stating that principle, the Court of Appeal continued, at para. 23:

> This approach to statutory interpretation -- sometimes referred to as the textual, contextual or purposive approach -- requires an examination of three factors: the language of the provision, the context in which the language is used and the purpose of the legislation or statutory scheme in which the language is found.

[71] The Applicants submit that the IPC's failure to interpret the notification requirement in a manner consistent its "text, context and purpose", as required by binding case law, was an error of law (in the context of Halton's appeal) and rendered the Decisions unreasonable (in the context of the judicial review applications).

[72] The Applicants say that the alleged "purposive" approach that the IPC adopted – that the "transformation" of the personal information amounted to "use" or "loss" – was animated by the desired outcome 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": SickKids Decision, at para. 52; see also Halton Decision, at para. 63. The Applicants argue that the IPC's construction of the statutory provision was guided by its conclusion that, in the face of "unauthorized action involving information that, in a fundamental sense belongs to them", notice to affected individuals must be provided: SickKids Decision, at para. 53; see also Halton Decision, at para. 64.

[73] The Applicant submit that to achieve the desired outcome, the IPC construed "used" and "lost" (being the terms that trigger a notice requirement) by recourse to a term – "transforms" or "transformation" – not employed in the contested provision. That is, the IPC relied on whether the information was "transformed" by the encryption rather than a genuine examination of the provision's text, context, and purpose. In considering "transformation" as a trigger for notice, the Applicants say that the IPC failed to properly construe the provision.

[74] As explained below, I do not agree that the IPC engaged in improper results-oriented reasoning in reaching the conclusion that notification was required.

[75] The Applicants based their argument on this issue on the narrow part of the Decisions where the IPC discussed the effect of the encryption when considering whether it amounted to a "use" or "loss" of the information within the meaning of the legislation. In doing so, the Applicants failed to consider the Decisions as a whole. They make no mention of many other pages of textual and contextual analysis in the Decisions: see for example, SickKids Decision, at paras. 13-39; Halton Decision, at paras. 18-62.

[76] Specifically, the Applicants take issue with the IPC's use of the term "transform" to explain why the encryption of containers of information was a "use" of that information. In doing so, the

Applicants do not consider the context in which the word "transforms" is used in the Decisions. In the SickKids Decision, at para. 40, the IPC stated:

> 40. … 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*. [Emphasis added.]

[77] In the Halton Decision, at para. 53, the IPC provided substantially similar reasoning with respect to the Halton attack.

[78] As discussed further below, the IPC used the term "transform" in the Decisions to explain the encryption process. It is worth noting that the IPC's explanation is essentially the same as both Applicants' responses to the IPC's notice of review: [1]

> As it pertains to ransomware, encryption is the process by which data is encoded or scrambled, rendering it unreadable and inaccessible to unauthorized users. This process converts data into a form that cannot be read without the conversion method (a "decryption key"). [Emphasis added. Footnotes omitted.]

[79] The IPC used the term "transform" rather than "convert". The words are synonymous.

[80] In the Decisions, the IPC tied its explanatory use of the term "transforms" back to the accepted legal test for determining whether the information was "used", that is, whether it had been "handled" (in SickKids's case) or "dealt with" (in both cases): see *PHIPA*, s. 2, definition of "use"; see also IPC, "Privacy, Part X of the *Child, Youth and Family Services Act*: A Guide to Access and Privacy for Service Providers" (May 2019), at p. 13.[2]

[81] In the SickKids Decision, at paras. 39-41, the IPC found that personal health information had been both "handled" and "dealt with". In the Halton Decision, at paras. 52-54, the IPC found that the personal information had been "dealt with". In both Decisions, the IPC found that the there had been an unauthorized "use" of the underlying information: SickKids Decision, at para. 42; Halton Decision, at paras 54-55. In doing so, the IPC rejected the Applicants' submission that the "locking (by encryption) of external containers housing personal health information has no effect on" the underlying information in the containers: SickKids Decision, at para. 40; Halton Decision, at para. 53. As explained further below, I see no error or unreasonableness in those findings.

---

[1] Response to Notice of Review (Representations from the Hospital), August 31, 2023, at p. 5, in Public Record of Proceedings between SickKids and the IPC, Tab 12A; Response to Notice of Review (Representations from Halton CAS), April 5, 2023, at p. 3, in Public Record of Proceedings between Halton and the IPC, Tab 11A.

[2] In that publication (cited in the Halton Decision, paras. 21, 38 and footnote 6,), the IPC provided guidance to service providers that "[g]enerally, **using** personal information means viewing or **dealing with** the information in a manner that does not include disclosing it" (emphasis added).

C. The Applicants have not established that the IPC erred or was unreasonable in finding there was an unauthorized use of personal information

[82] The Applicants submit that in the Decisions, the IPC erred and was unreasonable in finding that there was an unauthorised "use" of personal information.

[83] As noted previously, the Applicants take issue with the use of the term "transform" when referring to the encryption process.

[84] In the Decisions, the adjudicator provided her "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 [health] information unavailable and inaccessible to authorized users of that information": SickKids Decision, at para. 40; Halton Decision, at para. 53. In the SickKids Decision, at para. 42, the IPC further explained that "this use of information occurs whether or not the threat actor actually views or accesses … or exfiltrates" the information: see also Halton Decision, at para. 54, to similar effect.

[85] In the SickKids Decision, at para. 40, the IPC found that the effect of making the personal health information unavailable was "a kind of 'handling' of or 'dealing with' that information" in accordance with the definition of "use" in *PHIPA.* As a result of this unauthorized "use", the IPC found that the duty to notify in s. 12(2) of *PHIPA* applied: SickKids Decision, at para. 45.

[86] In the Halton Decision, at paras. 53-54, the IPC found that the effect of making the personal information unavailable to Halton was "a kind of 'dealing with' that information", which it found to be a "use" of the information within the meaning of the *CFSA.* As a result, of this unauthorized "use", the IPC found that the duty to notify in s. 308(2) applied: Halton Decision, at para. 56.

[87] In the Decisions, the IPC stated that it was adopting a "purposive" approach to interpretation of the notification requirement "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": SickKids Decision, at para. 52; Halton Decision, at para. 63. The IPC noted that it was consistent with the purposes of those statutory provisions that affected individuals be "notified of a third party's malicious action" denying the custodian or service provider access to the information. In the Sick Kids Decision, at para. 53 (and to similar effect in the Halton Decision, at para. 64), the IPC continued:

> 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. [Emphasis added.]

[88] The Applicants submit that the IPC's interpretation of "use" was not supported by the **text**, **context** or **purpose** of the statutory provisions. They say that the IPC's interpretation appears to have put the desired outcome – that a cyberattack of this nature requires notification to individuals – before a proper construction of the provision at issue.

[89] Regarding the **text** of the notification provisions, the Applicants submit that in order to fall within the term "use" in the notification provisions, the "threat actors" must have interacted with the information directly. The Applicants say that this requirement follows from the correct interpretation of the term "use", which requires consideration of whether the information has been "viewed" or "dealt with" or (in the case of *PHIPA*) "handled". The Applicants argue that the grammatical and ordinary sense of those terms support the conclusion that for the personal information to be "used" it must be interacted with directly. The Applicants say that interpretation of the notification requirement also requires consideration of the information custodian's obligations under s. 12(1) of *PHIPA* or s. 308(1) of the *CYFSA* to ensure that the records containing personal information are protected against "unauthorized copying, modification or disposal." The Applicants note that there is no evidence that the information in the containers had in any way been viewed, accessed, copied, or modified. In these circumstances, the Applicants submit that the requirement to notify individuals is not engaged.

[90] Regarding the **context** of the notification provisions, the Applicants submit that the notice requirement's purpose is to enable an individual to take protective steps to minimize the risk of harm of a privacy breach and to facilitate the exercise of their right to privacy by making a complaint to the IPC or by pursuing an action in Superior Court for actual harm stemming from the breach: see *PHIPA*, s. 65(1); *CYFSA*, s. 325(1). The Applicants argue that the attacks in question did not compromise the confidentiality of personal information or cause any harm to privacy interests. Therefore, there was nothing that needed to be rectified by way of a complaint or court proceeding. The Applicants says that finding a duty to notify in these circumstances is illogical and serves no purpose relevant to the objects of the provisions.

[91] Regarding the **purpose** of the notification provisions, the Applicants submit that the IPC's interpretation of "use without authority" does not accord with the purpose of the provisions. According to the Applicants, that purpose relates to the protection of the privacy interest of affected individuals, rather than requiring notification of cyber attacks that do not impact their privacy interest. The impact of the ransomware attack was to make the individuals' private information temporarily unavailable to the custodian or service provider. The Applicants say that there was little to no impact on the care or services they provided. They submit that in those circumstances, interpreting the attack as "use without authority" that triggers notification is not aligned with the objectives of the legislation and would impose an unnecessarily onerous burden on the Applicants.

[92] The OHA intervened in the judicial review applications and the appeal to support the Applicants' position. The OHA submits that it is not appropriate to adopt a broad duty to notify about ransomware attacks where individuals' data was not actually viewed, accessed or stolen by threat actors, and where the information was restored quickly such that all or almost all individuals were unaffected. The OHA says that it is important to avoid an interpretation of the requirement that results in useless, over-notification. They submit that such notifications do not advance the legislative purposes of protecting information confidentiality and personal privacy. Instead, such notifications can result in needless costs, can unnecessarily raise anxiety levels of affected individuals, and can lead to notification fatigue. The OHA says that avoiding an overly broad interpretation of the obligation to notify is particularly important where privacy legislation does

not include a risk-based threshold (such as a real risk of significant harm ["RROSH"]) for notification to be required.[3]

[93] I have concluded that the Applicants have not demonstrated that the IPC erred or was unreasonable in finding that there was an unauthorized "use" of personal information that gave rise a requirement to notify affected individuals.

[94] With respect to the **text** of the provisions, I am not persuaded by the Applicants' submission that the information must be interacted with directly in order for notification to be required. The Applicants base this argument on the obligation to take reasonable steps to protect against "unauthorized copying, modification or disposal": *PHIPA*, s. 12(1); *CYFSA*, s. 308(1). The Applicants submit that those terms are meant to exemplify "uses" involving direct interaction with personal information. On the contrary, those terms demonstrate the opposite, namely, that uses can occur without direct interaction with the information. For example, physically destroying a hard drive that contains personal information disposes of that information, without any direct interaction with that information itself.

[95] With respect to **context** and **purpose** of the provisions, I do not agree with the Applicants that the only purpose of notification is to allow individuals to take steps to minimize the risk of harm resulting from the privacy breach or make a complaint to the IPC and pursue an action in Superior Court for actual harm.

[96] As explained below, while many Canadian privacy statutes contain a risk-based threshold for notification, *PHIPA* and the *CYFSA* do not require that a risk of harm to the individual be established for notification to be required.

[97] First, Legislatures use clear statutory language (such as RROSH) to indicate a risk-based notification threshold: see e.g. *FIPPA*, s. 40.1. There is no such language in *PHIPA* or the *CYFSA*.

[98] Second, the Applicants appear to assume (wrongly) that complaints under *PHIPA* and the *CYFSA* can be filed only by individuals who have been notified of a breach and wish to complain about the theft, loss, or unauthorized use or disclosure of their personal information. Unlike other privacy and access to information statutes that expressly link the right to file a complaint with notification,[4] *PHIPA* and the *CYFSA* do not. Any individual may file a complaint with the IPC when they have reasonable grounds to believe that any of the requirements applicable legislation have been or are about to be contravened: see *PHIPA*, s. 56(1); *CYFSA*, s. 316(1). As well, the right to pursue an action in Superior Court is not tied to notification: see *PHIPA*, s. 65; *CYFSA*, s. 325.

[99] While there is no dispute that advising individuals of risks is an important reason for notification, it is not the fundamental or only purpose of notification. For example, individuals

---

[3] For example, see *FIPPA*, s. 40.1, which requires notification of a privacy breach based on the RROSH threshold, effective July 1, 2025: *Strengthening Cyber Security and Building Trust in the Public Sector A*ct, S.O. 2024, c. 24, Sched. 2, s. 6; see also *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 10.1(3).
[4] See *FIPPA*, ss. 40.1(4).

who are notified of a breach can complain to the IPC that the information custodian did not comply with the security obligations in s 12(1) of *PHIPA* or s. 308(1) of the *CYFSA*. Doing so allows individuals to hold information custodians accountable for how they are protecting the individuals' personal information.

[100] Another important purpose of the notification requirement is to enable the IPC to exercise its statutory authority to provide oversight of Ontario's access to information and privacy laws, including to determine whether to conduct a review under s. 58(1) of *PHIPA* and s. 318(1) of the *CYFSA*. The Applicants argue that a ransomware attack that encrypts containers containing personal information is not an unauthorized use or loss of such information. I agree with the IPC's submission that, if this argument were accepted by this court, it would unduly restrict the obligation imposed on information custodians to be transparent and accountable in relation to the expanding threat of cyber attacks of this nature. The absence of a requirement to notify in these circumstances also would interfere with the IPC's ability to ensure that information custodians conduct a proper investigation to determine whether individuals' personal information was compromised.

[101] I also disagree with the Applicants' submission (supported by the OHA) that interpreting the cyber attack as "use without authority" that triggers notification is not aligned with the objectives of the legislation and would impose an unnecessarily onerous burden on the Applicants. They also raise the spectre of "over-notification" and "notification fatigue".

[102] As the Decisions indicated, the IPC itself recognized that an "overly broad interpretation" of the notification requirement could lead to "notification fatigue on the part of the public, disproportionate costs to the [information custodian], and other unintended and undesirable consequences": SickKids Decision, at para. 51; Halton Decision, at para. 62. However, the IPC went on find that the notification requirement was triggered in this case, adopting a "purposive" approach to interpretation of the provisions: SickKids Decision, at paras. 52-53; Halton Decision, at paras. 63-64. It is notable that the IPC characterized the purpose of notification as "to inform individuals of unauthorized activities involving information that, in a fundamental sense, belongs to them": SickKids Decision, at para. 53; Halton Decision, at paras. 64.

[103] In doing so, the IPC recognized that affected individuals have a legitimate continuing interest in what happens to that information, which justifies notification for purposes beyond being alerted to risks of harm. This approach is consistent with other provisions of *PHIPA* and the *CYFSA*, which require notification of affected individuals if the information custodians use or disclose information contrary to their written public statements, even when they would be otherwise be legally authorized to use or disclose the information under those statutes: see *PHIPA*, s. 16; *CYFSA*, s. 311. That notification requirement is not tied to risk of harm. Rather, it recognizes the individuals' continuing interest in their personal information and in ensuring that information custodians are transparent and accountable.

[104] Accordingly, I conclude the Applicants have not demonstrated that the IPC erred or was unreasonable in finding that there was an unauthorized "use" of personal information that gave rise a requirement to notify affected individuals. As a result, I conclude that the IPC did not err and was reasonable in finding that the Applicants were required by s. 12(2) of *PHIPA* or s. 308(2)

of the *CYFSA* to notify individuals of the relevant ransomware attack. It follows that the judicial review applications and the appeal should be dismissed on the merits.

D. Loss of information

[105] The Applicants submit that in the Decisions, the IPC erred and was unreasonable in finding that there was a loss of personal information. The Applicants say that the IPC's conclusion that the temporary unavailability or inaccessibility amounted to loss leads to a flawed result and does not accord with a proper consideration of the text, context and purpose of s. 12(2) of the *PHIPA* and s. 308(2) of the *CYFSA*.

[106] In support of their position relating to the interpretation of the term "loss", the Applicants make submissions that are essentially similar to the ones they make to support their position that the IPC erred and was unreasonable in finding that there was an unauthorized "use" of personal information. Suffice it to say that I find those submissions equally unpersuasive when considering whether the IPC erred or was unreasonable in its interpretation of the term "loss" in those provisions. Since I have already found the Applicants have not met their burden of establishing error or unreasonableness in the IPC's finding that the was an unauthorized use of personal information, it is unnecessary to consider further whether there was error or unreasonableness in finding there was a loss of personal information. Notification of affected individuals and the IPC would be required on either basis.

V. Disposition

[107] For the above reasons, I would dismiss the appeal and the judicial review applications. As the parties agreed, I would not make a costs order.

_____
Lococo J.

I agree: _____
Sachs J.

I agree: _____
A.D. Kurke J.

Date: September 16, 2025

CITATION: Hospital for Sick Children v. Ontario (Information and Privacy Commissioner), 2025 ONSC 5208
DIVISIONAL COURT FILE NO.: 449/24, 450/24 & 453/24
DATE: 20250916

ONTARIO

SUPERIOR COURT OF JUSTICE

DIVISIONAL COURT

Sachs, Lococo and A.D. Kurke JJ.

BETWEEN:

THE HOSPITAL FOR SICK CHILDREN
Applicant

– **and** –

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
Respondent

– **and** –

ONTARIO HOSPITAL ASSOCIATION
Intervenor

AND BETWEEN

HALTON CHILDREN'S AID SOCIETY
Applicant/Appellant

– **and** –

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
Respondent

REASONS FOR JUDGMENT

R. A. LOCOCO J.

Date: September 16, 2025