Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 254

File HR21-00270

Kingston, Frontenac and Lennox & Addington (KFL&A) Public Health

July 5, 2024

Summary: In June 2021, the respondent Kingston, Frontenac and Lennox & Addington Public Health (KFL&A) was the subject of a ransomware attack. The attack resulted in the encryption of multiple KFL&A servers, including those containing personal health information.

The IPC initiated a review of the matter under the *Personal Health Information Protection Act, 2004* (*PHIPA*). Section 12(2) of *PHIPA* sets out a duty on health information custodians like KFL&A to notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or used or disclosed without authority. KFL&A takes the position that the threat actor's encryption of servers containing personal health information, without evidence of any access to or exfiltration of that information, does not qualify as a theft, loss, or unauthorized use or disclosure of personal health information within the meaning of section 12(2), and that the duty to notify does not apply.

In this decision, the adjudicator finds that the threat actor's encryption of KFL&A servers affected the personal health information in those servers, by making that information unavailable and inaccessible to authorized users. The ransomware attack resulted in both an unauthorized use and a loss of personal health information within the meaning of section 12(2). As a result, KFL&A had a duty under *PHIPA* to notify affected individuals "at the first reasonable opportunity." At the time of the incident, KFL&A issued media releases informing the public about the attack, and of the progress of its recovery efforts. While KFL&A's notice did not comply with section 12(2) because it did not include a statement about the right to complain to the IPC, and ought to have included more detail for the benefit of affected individuals, the adjudicator finds no useful purpose in directing that further notice be given now. She concludes the review without issuing an order.

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

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

OVERVIEW:

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

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

[3] This decision concerns a ransomware encryption attack on Kingston, Frontenac and Lennox & Addington Public Health (KFL&A), a health information custodian within the meaning of *PHIPA*.[2] For the reasons that follow, I find that an unauthorized third party's encryption of KFL&A servers containing personal health information resulted in the unauthorized use and loss of that information within the meaning of section 12(2) of *PHIPA*. As a result, KFL&A had a duty to notify affected individuals at the first reasonable opportunity. At the time of the incident, KFL&A posted media releases on its website, informing the public about the attack and the progress of its recovery efforts. While these notices did not comply with the requirement in section 12(2) to include a statement about the right to complain to the IPC, and ought to have included additional detail for the benefit of affected individuals, in the circumstances I find no useful purpose in directing

[1] PHIPA Decisions 253 and 255, and CYFSA Decision 19.
[2] Specifically, the medical officer of health of the board of health governing KFL&A is the health information custodian (paragraph 6 of section 3(1) of *PHIPA*).

that further notice be given now. I conclude the review without making an order.

BACKGROUND:

[4] Around June 14, 2021, an unauthorized third party (the threat actor) gained access to KFL&A's IT systems. KFL&A became aware of the incident on June 25, 2021, when it noticed an increase in user VPN login issues and discovered that several servers were inaccessible. KFL&A later learned that the ransomware attack resulted in the encryption of its servers and backups, as well as some workstations. At the time of the attack, the threat actor also claimed to have exfiltrated files containing personal health information, as well as financial and HR records.

[5] KFL&A retained external legal counsel and a forensic firm to investigate the attack and to conduct ransom negotiations. It also reported the matter to law enforcement, and to the Office of the Information and Privacy Commissioner of Ontario (IPC). The IPC opened the present file to address this matter.

[6] KFL&A advised the IPC that its forensic investigation found "indication of compromise" on several KFL&A systems and servers, a number of which contained personal health information. While the investigation found tools associated with exfiltration in some of the servers containing personal health information, it ultimately determined there was no evidence the threat actor had gone through with exfiltration. Based on the findings of the investigation, KFL&A also concluded that no personal health information was "viewed, opened, or otherwise affected" as a result of the attack. However, KFL&A confirmed that the threat actor encrypted over 8,000 patient records on its server. Following payment of a ransom, a decryption key was obtained, and KFL&A reports that "all important data was successfully decrypted."

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

[8] However, this matter proceeded to adjudication to address outstanding issues arising from KFL&A's position that the ransomware attack did not give rise to the duty to notify affected individuals. I decided to conduct an IPC-initiated review of this matter under section 58(1) of *PHIPA*. Section 58(1) permits the IPC to conduct a review of any matter, on its own initiative, where it has reasonable grounds to believe that a person has contravened or is about to contravene a provision of *PHIPA* or its regulations.

[9] During the review, I sought and received representations from KFL&A on whether

the ransomware encryption event resulted in the theft, loss, or unauthorized use or disclosure of personal health information, within the meaning of those terms in section 12(2) of *PHIPA*, and, if so, the appropriate form of notice in the circumstances.[3]

[10] Consistent with the practice I have adopted in the other decisions I am releasing on this date, I have wherever possible left out references in this decision to the specifics of KFL&A's security safeguards.[4]

ISSUES:

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

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

DISCUSSION:

[11] Among other purposes, *PHIPA* sets out rules to ensure the security of "personal health information" that is in the "custody" or "control" of a health information custodian.[5]

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

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

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

---

[3] I also asked KFL&A to comment on the potential relevance to my review of IPC Orders HO-004 and HO-007. In those orders, the IPC endorsed the strong encryption of mobile devices as a potentially effective means of mitigating the risks associated with having personal health information accessed outside normal network protections. While KFL&A 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 have not relied on these IPC orders in making my determinations in this decision.

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

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

custody or control. This section states:

> A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

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

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

> Subject to subsection (4) [which is not applicable in the circumstances of this file] and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,
>
> (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
>
> (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

[16] Despite its public communications about the ransomware attack, KFL&A took the position that the duty to notify in section 12(2) of *PHIPA* does not apply, based on its conclusion that the threat actor did not view, access, or exfiltrate any personal health information when it encrypted KFL&A servers containing that information. KFL&A asserts that the encryption of its servers, and of the files of personal health information on those servers, does not qualify as a theft, loss, or unauthorized use or disclosure of personal health information triggering the duty to notify.

[17] Even assuming the threat actor did not view, access, or exfiltrate any personal health information, it is my finding that the threat actor's encryption of personal health information, by itself, qualifies as both an unauthorized use and a loss of that information within the meaning of section 12(2) of *PHIPA*. My reasons follow.

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

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

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

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

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

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

Disclosure

[22] KFL&A states that despite the threat actor's initial claims, its forensic investigation found no indication that personal health information was exfiltrated by the threat actor.[7] I understand this to be the basis for KFL&A's position that there was no disclosure of personal health information as a result of the ransomware attack.

[23] A determination that there was no exfiltration may support a finding that the

---

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

[7] KFL&A explains that to arrive at this conclusion, its forensic investigation team analyzed potentially affected folders and files, including for evidence of tools normally used for exfiltration, reconnaissance tools, and ransomware binaries.

ransomware attack did not result in any *further* disclosure of personal health information by the threat actor (for example, to the dark web or to any other person). However, I shared with KFL&A a preliminary view that the threat actor's access to (infiltration of) KFL&A's information systems, by itself, qualifies as a "disclosure" by KFL&A to the threat actor of personal health information contained in the affected information systems, whether or not KFL&A intended to disclose that information or was even aware of the threat actor's actions.[8]

[24] Because of my findings below, it is unnecessary to make a finding on whether the threat actor's infiltration of KFL&A's information systems, on its own, qualifies as a "disclosure" of personal health information within the meaning of *PHIPA*, and I decline to do so. I note that I accept KFL&A's evidence that there has been no exfiltration—and thus, no further disclosure by the threat actor—of personal health information that was contained in the information systems affected by the ransomware attack.

Use

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

[26] KFL&A says that while the threat actor encrypted over 8,000 patient records containing personal health information, there is no evidence of any access to personal health information. I understand KFL&A to be saying there is no evidence the threat actor accessed (for example, by viewing or opening) any specific patient record when it encrypted thousands of these records in the course of the ransomware attack.

[27] KFL&A submits that the encryption of records of personal health information, without evidence of specific access to or exfiltration of that information, is not a "use" of personal health information. KFL&A offers an analogy to paper files stored in cabinets within a locked shed. It says the encryption event that occurred here is like a threat actor who jumps over a fence and puts an extra padlock on the shed, without entering the shed. I understand KFL&A to be saying that the locking (by encryption) of a server—and by extension, the encryption of the patient records housed on the server—does not, by itself, affect the personal health information in the records in a way that would qualify as a "use" of that information.

[28] For the purposes of this decision, I am prepared to accept KFL&A's evidence that the threat actor did not access (for example, by viewing or opening) any particular patient record when it encrypted KFL&A servers and thousands of patient records stored on those servers. However, the question remains whether the personal health information in the encrypted records was "handled" or "otherwise dealt with," and thus "used" within the

[8] In this context I noted the potential relevance of some IPC decisions (including PHIPA Decisions 49 and 110) in which the IPC concluded that the custodian had "disclosed" personal health information within the meaning of *PHIPA*, by releasing or making available that information to the unauthorized third party, despite the custodian's lack of intention to share that information with the unauthorized party.

meaning of *PHIPA*. I find that the personal health information was used in this way.

[29] This is because I do not accept the premise that the encryption of records of personal health information has no effect on that information. Instead, it is my view that the act of encryption transforms that personal health information—at a minimum, by making it unavailable and inaccessible to authorized users of the information. The effect of making unavailable to KFL&A the personal health information in the encrypted patient records, to use, disclose, and otherwise handle for authorized purposes, is a kind of "handling" of or "dealing with" that information, and thus a use of that information within the meaning of *PHIPA*.

[30] This use of personal health information occurs whether or not the threat actor actually opens or views specific records of personal health information, or exfiltrates that information outside KFL&A's environment. It is my finding that the act of encrypting records of personal health information is, by itself, a use of that information within the meaning of *PHIPA*.

[31] 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 KFL&A servers and the patient records housed on those servers was an unauthorized use of personal health information within the meaning of section 12(2).

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

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

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

[34] The duty to notify in section 12(2) also arises in the event personal health information in the custody or control of a custodian is lost.[9] There is no definition of "lost"

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

or "loss" in *PHIPA*.

[35] KFL&A relies on the submissions described above to support its position that there was no loss of personal health information. KFL&A also observes that following the payment of a ransom, a decryption key was obtained and "all important data was successfully decrypted."

[36] By employing the decryption key, KFL&A was able to regain access to the data, including personal health information, encrypted by the threat actor, and to resume its functions as a health unit. However, the successful recovery of that information does not negate the fact that, for some period of time, personal health information in the custody or control of KFL&A was made inaccessible to it as a result of the threat actor's attack on its information systems. Specifically, the threat actor's encryption of KFL&A servers had the effect of denying authorized users (i.e., KFL&A) access to personal health information that it required to provide services. 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.

[37] 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.

[38] 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.

[39] 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).[10] The different outcomes in these different scenarios are in keeping with the purposes of the duty to notify in *PHIPA*.

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

[40] My findings of unauthorized use and loss of personal health information do not necessarily lead to a conclusion that KFL&A failed in its duty under *PHIPA* to take reasonable steps to protect the personal health information in its custody or control [section 12(1)]. The IPC has long recognized that the duty in section 12(1) of *PHIPA* to take "reasonable" steps does not call for perfection, and that there is no detailed prescription in *PHIPA* for what is reasonable.[11] Moreover, in the context of similar obligations on institutions under *FIPPA* and *MFIPPA*,[12] 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.[13] The requirement to take reasonable steps to protect personal health information does not call for a guarantee against cyberattacks or other threats of unauthorized use or loss of personal health information.

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

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

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

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

---

[10] Assuming, of course, that the custodian is able to regain access to personal health information after these events are complete.

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

[12] 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."

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

individual's right to complain to the IPC [paragraph (b)].

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

[45] 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.

[46] 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.

[47] In this case, KFL&A took prompt steps to investigate and contain the cyberattack, including by engaging third-party forensic experts, notifying law enforcement, and fully cooperating with the IPC in this review. I have taken into account the very large number of individuals who were affected by the attack, and KFL&A's submission that the personal health information affected by the attack was relatively limited, and of a less sensitive nature than the kind of information typically appearing in complete patient files.[14] At the time of the incident, KFL&A issued two "community awareness media releases" about the cyberattack, and its remediation efforts in response. There was also local media coverage of the incident.

[48] While the KFL&A's communications served the purpose of informing the public about the attack, they failed to notify affected individuals about the right to complain to the IPC, as required by section 12(2)(b) of *PHIPA*. These communications also should have included more details about the types of personal health information affected by the attack, and provided contact information for a person at KFL&A who could answer

[14] KFL&A explains that the patient information stored on its servers consisted of snippets of information from patient files, and not entire patient files. These snippets consisted of information that could not be saved to provincial databases—for example, screening tool forms, consent forms, and correspondence about following up on screenings and assessments.

questions from affected individuals.

[49] However, through this IPC-initiated file, the IPC has considered issues under *PHIPA* arising from the ransomware attack, including the sufficiency of KFL&A's responses and its notification obligations. Considering the overall circumstances, including the passage of time, I find there is no useful purpose in directing that further notice be given now. I therefore conclude the review without making an order.

NO ORDER:

For the foregoing reasons, I find that the June 2021 ransomware attack on KFL&A servers containing personal health information resulted in an unauthorized use and a loss of personal health information within the meaning of section 12(2) of *PHIPA*. As a result, KFL&A had a duty to notify affected individuals at the first reasonable opportunity of the breach.

While KFL&A's notice of the breach did not comply with section 12(2) because it did not include a statement about the right to complain to the IPC, and ought to have included more detail for the benefit of affected individuals, in the circumstances I find no useful purpose in directing that further notice be given now. I conclude the review without issuing any order.

Original signed by: July 5, 2024

Jenny Ryu
Adjudicator