Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 284

Complaints HR23-00500, HR23-00501, HR23-00502, HR23-00503, HR23-00504, HR23-00521

Bluewater Health, Chatham-Kent Health Alliance, Erie Shores HealthCare, Hôtel-Dieu Grace Healthcare, Windsor Regional Hospital, The Tilbury District Family Health Team

June 16, 2025

Summary: Five hospitals and a health care clinic (collectively, the custodians) reported a privacy breach under the *Personal Health Information Protection Act, 2004* (the *Act*) involving a ransomware attack against their network operated by a shared IT service provider. The threat actor exfiltrated electronic records containing personal health information of hundreds of thousands of patients and encrypted many network servers. After discovering the attack, the service provider shut down its network and engaged security and forensic experts. The threat actor published the stolen files. The custodians issued public releases about the incident and notified patients whose personal health information was stolen.

The threat actor launched its attack by leveraging the network's administrative accounts. A forensic investigation could not determine how these accounts were compromised.

To remediate the incident, the service provider implemented additional safeguards to reinforce the security of its systems, including increased detection measures, traffic restrictions and multi-factor authentication.

In this decision, the investigator finds that the data exfiltration was an unauthorized use and disclosure of personal health information. He also finds that the hostile encryption of the servers resulted in an unauthorized use and loss of personal health information of the custodians' patients and, therefore, the custodians were required to notify the affected patients as required by section

12(2) of the *Act*. The investigator finds that, although the custodians did not notify as required, there is no useful purpose in ordering additional notification in this case.

In light of the measures taken to contain, investigate and remediate the incident, the investigator finds that the custodians have responded adequately to the breach and concludes that a review of this matter under Part VI of the *Act* is not warranted.

Statutes Considered: *Personal Health Information Protection Act, 2004,* S.O. 2004, c. 3, sections 10(1), 10(2), 12(1), 12(2), 30(2) and 30(3)

Decisions Considered: PHIPA Decisions 110, 210, 253, 254 and 266

Cases Considered: *LifeLabs LP v. Information and Privacy Commissioner (Ontario),* 2024 ONSC 2194 (CanLII)

INTRODUCTION:

[1] On October 27, 2023, the following five hospitals (collectively, the hospitals) reported a privacy breach under the *Personal Health Information Protection Act, 2004* (the *PHIPA* or the *Act*) to the Office of the Information and Privacy Commissioner of Ontario (the IPC):

- Bluewater Health (BWH)
- Chatham-Kent Health Alliance (CKHA)
- Erie Shores HealthCare (ESHC)
- Hôtel-Dieu Grace Healthcare (HDGH)
- Windsor Regional Hospital (WRH)

[2] The breach involved a ransomware cyberattack which targeted the hospitals' shared third-party service provider, TransForm Shared Service Organization (TSSO).

[3] On November 6, 2023, the Tilbury District Family Health Team (TDFHT or the clinic), a community health care clinic based in Tilbury, Ontario, also reported the same breach to the IPC.

[4] In this decision, the hospitals and the clinic are collectively referred to as the "custodians". The custodians are represented by the same legal counsel who reported the breach on their behalf. Since the incident directly involved TSSO as the custodians' shared service provider, I have prepared one decision in respect of all custodians.

[5] During the early resolution stage of the IPC's *PHIPA* complaint process, counsel provided details of the breach and steps that were taken in response. After review of the information, the files were moved to the investigation stage, and I was assigned as the

investigator. As part of my investigation, I requested and received written representations from the custodians.

[6] In this decision, I find that the threat actor's exfiltration of data amounted to unauthorized use and disclosure of personal health information of patients of the six custodians and therefore a breach under the *Act*. I also find that the threat actor's hostile encryption resulted in unauthorized use and loss of personal health information of their patients.

[7] With respect to notification, I find that although the custodians appropriately notified individuals affected by the data exfiltration, they were also required to notify those affected by the hostile encryption, which they did not. Despite this finding, I decide that there is no useful purpose in ordering additional notification at this stage.

[8] Finally, given the custodians' containment and remediation of the incident, including measures implemented to improve the security of the systems and related procedures and practices, I find that they have responded adequately to the breach and that a review under Part VI of the *Act* is not warranted.

BACKGROUND:

[9] The five hospitals serve residential communities at various locations in southwestern Ontario, providing a diverse range of health care programs and services, including but not limited to specialties such as internal medicine, surgery and advanced care.

[10] TDFHT is a group of health care professionals, including family doctors, nurse practitioners, nurses, social workers, pharmacists, dieticians and others, serving patients in Tilbury, Ontario and surrounding areas.

[11] TSSO is a non-profit organization and a shared third-party service provider for medical institutions in southwestern Ontario. TSSO was founded by the hospitals, who provide TSSO with funding, and their executive members serve as part of the organization's board of directors. In turn, TSSO provides a special suite of services to the hospitals, including the provision and maintenance of a central network which houses core applications essential for their operations. At the time of the attack, nearly all of those applications were housed together within one segmented portion of the TSSO network.

[12] A separately segmented portion of the network was used to support BWH's on-premises electronic medical record (EMR) system which allowed BWH's third-party vendor to access the network directly to provide related services including maintenance. The segmented BWH portion and the rest of the TSSO network are interconnected and accessed via secure virtual private networks (VPNs).

[13] To its clients aside from the hospitals, TSSO also provides network infrastructure and other hosting services, application support and maintenance. TDFHT, as a client, relied on TSSO for its core IT and network system and other services such as corporate shared drives and email hosting. TDFHT utilized a different service provider for its EMR system.

The incident

[14] In the late evening of October 22, 2023, TSSO began receiving reports from its network users having issues with slow response or with logging into applications. Shortly after, remote logins into the TSSO environment began failing. The TSSO network team was engaged, followed by on-site attendance of a local system administrator at TSSO's regional data centre. However, the problem could not be diagnosed at that time.

[15] In the early hours of October 23, the administrator discovered within the network a ransomware note from an unauthorized actor (the threat actor). TSSO engaged its incident response plans and executive escalation protocols. Twenty minutes later, TSSO disconnected the network from the Internet and placed the network on standby pending a forensic investigation.

[16] TSSO's investigation revealed that the threat actor successfully infiltrated the network by leveraging compromised administrator account credentials. The threat actor not only exfiltrated data, but also encrypted a significant number of network assets, preventing their operations and access to stored data. The attack did not impact networks not managed by TSSO, including electronic systems hosted locally at each of the hospitals and the clinic.

[17] At the start of the attack, the threat actor published lists of the exfiltrated files. TSSO and the hospitals declined to pay the ransom. In November 2023, the threat actor published the exfiltrated data in the dark web.

[18] The incident had a systematic impact on the operations of all of the custodians, most significantly the hospitals. Each of the hospitals initiated a Code Grey and entered downtime procedures. TDFHT also implemented its incident response protocol. The custodians maintained regular communications with TSSO regarding the circumstances of the breach and status of the internal investigation into cause and scope.

[19] To contain the incident, TSSO shut off the network's connections including VPN access and all Internet access for TSSO managed hospitals/customers, and all accounts were disabled and/or locked out and subjected to forced password reset.

[20] After securely erasing and reformatting the encrypted servers, TSSO successfully restored most of its services to the hospitals, including all core clinical services such as the EMR, communication and payroll systems. IT services were safely restored for TDFHT.

PRELIMINARY ISSUES:

[21] There is no dispute, and I find, that the custodians are each a "health information custodian" as defined under section 3(1) of the *Act.*

[22] It is also not in dispute that TSSO is the custodians' agent as defined under section 2 of the *Act.*[1] As the custodians' shared third-party provider of information architecture and other IT services, TSSO directly responded to the breach, worked with and informed the custodians regarding steps to contain and remediate the incident. I note also that the hospitals' shared service agreement with TSSO explicitly describes TSSO as their agent (as defined under the *Act* and with corresponding responsibilities under the *Act*) when it accesses personal health information.

[23] Furthermore, it is not in dispute that the electronic files on the TSSO network that were *exfiltrated* by the threat actor contained personal health information (as defined under section 4(1) of the *Act*) in the custody or control of each custodian, and that the exfiltration was an unauthorized use and disclosure of personal health information which triggered the requirement under section 12(2) to notify the affected individuals.

[24] However, what is in dispute is whether the threat actor's *encryption* of network servers, by itself, was a theft, loss, or unauthorized use or disclosure of personal health information. The custodians take the position that, in the circumstances where the encryption alone occurred without exfiltration, and with full restoration from back ups, the encryption did not amount to a theft, loss, or unauthorized use or disclosure and therefore, the custodians were not required to notify individuals whose information was affected solely by encryption. I will address this issue further below.

Forensic report

[25] During this investigation, I requested that the custodians produce a copy of the forensic report that was prepared or obtained as part of investigating the incident, including any root cause analysis report. I also asked for a copy of any forensic report describing the ransomware encryption deployed within the TSSO network.

[26] Counsel identified a single forensic report as responsive to these requests and initially declined my request to produce it based on claims of legal privilege, submitting that the report was created for the dominant purpose of preparing for existing litigation

[1] Section 2 of the *PHIPA* provides the definition as follows: "agent", in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated.

and informing solicitor advice. However, counsel also noted that the custodians recognized the IPC's authority to seek facts pertinent to its investigation and would respond to all factual inquiries.

[27] I requested that the custodians reconsider the IPC's request for production of the forensic report. I provided reference to *LifeLabs LP v. Information and Privacy Commissioner (Ontario)*, a recent decision of the Ontario Divisional Court which rejected the health information custodian's claims of privilege over facts concerning the privacy breach, its investigation and remediation.[2]

[28] Counsel eventually provided the IPC with a copy of the forensic report and submitted that the contents of the report are "purely factual in nature". Counsel also acknowledged that as a result, the custodians would be obliged to produce all of the contents of the report to the IPC.

[29] However, counsel also stated that the report was being produced solely for the purposes of the IPC's investigation and without any waiver of solicitor-client and litigation privilege. He submitted that the facts contained in the forensic report have been supplied through other means, presumably referring to submissions the custodians provided to the IPC directly in response to questions posed during the investigation.

[30] I acknowledge that during this investigation, the custodians provided the IPC with factual details regarding the circumstances of the breach obtained through forensic experts. The custodians did not claim privilege over the factual information provided in response to the IPC's inquiries.

[31] After reviewing the forensic report, I determined that in writing this decision, I only need to refer to the information which the custodians provided as part of the IPC's investigation, and not the information which is found exclusively in the forensic report. Accordingly, I do not need to make a determination with respect to the custodians' claims of privilege over the forensic report itself. However, I will comment briefly on the relevant authority on this issue and clarify the IPC's general position on the production of forensic reports in the context of a privacy breach under the *Act*.

[32] *LifeLabs* related to a 2019 cyberattack incident in which the threat actor obtained personal health data of millions of Canadians and demanded a ransom payment. The IPC, in a joint investigation with the British Columbia Office of the Information and Privacy Commissioner (BC IPC), sought information from LifeLabs, some of which was contained in reports prepared for LifeLabs by third party consultants, including a forensic investigation report prepared by a cybersecurity firm hired by LifeLabs. LifeLabs resisted production of these documents, and claimed privilege over the reports, as well as the factual information in the reports. LifeLabs sought judicial review of a joint decision of the IPC and BC IPC which rejected LifeLabs' claims of privilege over documents related

[2] *LifeLabs LP v. Information and Privacy Commissioner (Ontario),* 2024 ONSC 2194 [*LifeLabs*], leave to appeal refused (22 November 2024), CoA-24-OM-0161 (ONCA).

to the breach and the facts in those documents.

[33] The Ontario Divisional Court dismissed the judicial review application. The court held that the IPC did not err in finding that facts concerning the investigation and remediation of the data breach are producible.[3]

[34] The court rejected the claim of litigation privilege on the basis that it does not apply to facts or "base information", even if those facts might also play a role in defending against parallel civil litigation.[4]

[35] The court further held that solicitor-client privilege does not extend to protect facts that are required to be produced pursuant to the IPC's statutory duty under the *Act* to investigate.[5] The court agreed with the statement in the IPC and BC IPC's joint decision on LifeLabs' claims of privilege that:

> Even if the communication is privileged, the facts referred to or reflected to [sic] in those communications are not privileged if they exist outside the documents and are relevant and otherwise subject to disclosure.[6]

[36] *LifeLabs* makes clear that, pursuant to the IPC's statutory mandate under the *Act,* relevant facts concerning the circumstances of a breach and their investigation, such as facts found in the forensic investigation report, are producible in response to the IPC's statutory power to obtain them, regardless of whether the report was obtained through legal counsel.

[37] As stated above, and for the purposes of the present decision, I need not refer to any information found exclusively in the forensic report. Accordingly, I make no findings with respect to the claims of privilege advanced in this case with respect to the report.

ISSUES:

[38] In this decision, I address the following issues:

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

2. If the notification requirement applies, was notice given in compliance with section 12(2)?

3. Did the custodians take reasonable steps to protect personal health information?

---

[3] *Ibid.* at para 84.
[4] *Ibid.* at paras 77-79.
[5] *Ibid.* at paras 80-84.
[6] *Ibid.* at para 80.

RESULTS OF THE INVESTIGATION:

[39] Before considering the above issues, I will first discuss how the threat actor executed the cyberattack, and the scope of personal health information that was affected as a result.

[40] During the IPC's investigation, the custodians provided technical details related to the cyberattack and TSSO's systems. The custodians requested that the IPC keep confidential certain details for security reasons given their sensitive nature. As such, I have omitted reference to some details or generalized them as necessary.

How the attack happened

[41] According to the custodians, the threat actor infiltrated the TSSO network by leveraging three compromised administrator accounts associated with the network.

[42] First, the threat actor leveraged one administrator account to establish external VPN connection to the network. This account held privileges that allowed access to the entire TSSO network. The threat actor initially entered the network at the segmented portion dedicated to BWH.

[43] The threat actor was able to then "live off the land"; in other words, by gaining access to the network using a legitimate account, the threat actor was able to avoid detection. Eventually, the threat actor used the same account to move and infiltrate deeper into other parts of the TSSO network.

[44] The threat actor accessed and extracted data from a portion of a shared network drive that was utilized by the custodians for various purposes (the Shared Drive).

[45] The IPC asked the custodians to describe the controls that were in place to regulate access to the Shared Drive. The custodians responded that TSSO sets and manages the Shared Drive's access permissions at the user level. Users for one organization are not granted access to another organization's shared folders, unless it is specifically requested as part of a cross-institutional endeavour. This type of access is rarely permitted and must be specifically requested by a hosting institution before access is granted to the requesting institution's users.

[46] The threat actor used a different administrator account to target the data of BWH specifically. They exfiltrated patient data from two locations: a database containing registration data of all BWH patients (the Database Report), and a server containing BWH's scan images (the Scan Drive).

[47] Finally, the threat actor used a third administrator account (which had access to controls over the local operating system of the overall TSSO network) to deploy a script which automatically encrypted the network's virtual server infrastructure. This resulted in the encryption of 192 virtual servers, many of which were application servers that

supported the hospitals' clinical care and diagnostic testing procedures. Other servers affected were used to support back-office administrative functions.

[48] At the time of the attack, the three administrator accounts used to infiltrate the TSSO network were not equipped with multi-factor authentication (MFA). The custodians submitted that the forensic investigation was unable to determine how these accounts had their credentials compromised. However, based on the information provided, the compromise of these administrator accounts played a pivotal role in enabling the ransomware attack.

Scope of exfiltration

[49] The custodians informed the IPC that the raw amount of data exfiltrated from the Database Report, the Scan Drive and the Shared Drive exceeded 150 GB in size, and confirmed that the threat actor published all exfiltrated data on the dark web. Below, I briefly describe the information taken from each of these three locations.

Database Report

[50] The Database Report included registration information of about 5.6 million visits by every patient seen at BWH or its predecessors since 1992, or approximately 267,000 patients. BWH's predecessor institutions are Lambton Hospitals Group, Charlotte Eleanor Englehart Hospital of Bluewater Health, Sarnia General Hospital, and St. Joseph's Hospital.

[51] According to BWH, the Database Report included different combinations of the following types of information:

- Name;
- Address;
- Contact information;
- Date of birth;
- Basic demographic information;
- Reason for health visit; and
- General notes on prior registration.

[52] BWH also determined that the Database Report included social insurance numbers (SINs) for approximately 20,000 of the total patients affected. Counsel submitted that since 2002, BWH was required to collect SINs from patients seeking treatments related to Workplace Safety and Insurance Board (WSIB) claims to properly process these claims. Counsel submitted that BWH collected SINs to enable Workers Compensation Board's,

and later WSIB's, record management protocols. However, counsel confirmed that SIN collection was not authorized by any statute or regulation.

[53] Counsel also informed the IPC that BWH collected SINs from non-WSIB patients between 1999 and 2006. However, the hospital was unable to locate former department leaders who were employed in 2006 and was unable to determine the reason for this practice.

Scan Drive

[54] The Scan Drive contained many images related to BWH's clinical and administrative functions. These images included:

- Oncology treatment records;
- Registration documents;
- Interoperative photos;
- Wounds and intraoperative colonoscopy photos;
- Urology and respiratory test reporting;
- Medication and appliance voucher receipts;
- OHIP and secondary insurance company notifications;
- Residential withdrawal management patient charting;
- Discharge charts;
- Financial information related to co-payments;
- Insurance reimbursement information; and
- Patient identification documents.

Shared Drive

[55] The threat actor exfiltrated a relatively small portion of the Shared Drive. The precise files taken were identified with the assistance of a third-party data mining vendor.

[56] The records exfiltrated from the Shared Drive varied for each custodian. Some custodians stored records related to operational activities such as meeting minutes and agendas, departmental communications and other business documents. Others stored clinical records with personal health information, including, but not limited to, patient registration and appointment lists, immunotherapy lists, vaccination lists, medication

summaries, infection control reports, transportation services booking requests, and billing and treatment cost information lists.

[57] Across the six custodians, the threat actor exfiltrated from the Shared Drive combinations of the following types of personal health information of patients:

- Name;
- Contact information (including phone number, mailing address and/or email address);
- Date of birth;
- Incidental health reference (e.g. appointment information);
- Treatment information/diagnosis (including clinic location);
- Treatment information;
- Prescription information;
- Medical record number;
- Patient ID;
- Health card number;
- Health insurance information; and
- Treatment cost information.

[58] Overall, the following number of patients had their records of personal health information taken from the three locations noted above:

Bluewater Health	267,000
Chatham-Kent Health Alliance	70,526
Erie Shores HealthCare	101,603
Hôtel-Dieu Grace Healthcare	15,456
Windsor Regional Hospital	29,051
Tilbury District Family Health Team	32,383

[59] In addition to the above figures, CHKA, ESHC and HDGH reported that information specific to their employees stored in the Shared Drive was also exfiltrated. The targeted

information included combinations of the employees' SINs, credit/debit card numbers, professional license numbers, and/or employee identification numbers.

[60] Pursuant to the definition of personal health information under section 4(1), the *Act* applies to records of personal health information that relates to an individual's health or to the provision of health care. Any other information about an individual that is included in a record containing personal health information is also included in the definition of a record subject to the *Act*.[7] However, employee records of a custodian used primarily for purposes other than providing health care are excluded from the definition of personal health information.

[61] I am satisfied that in this case, the exfiltrated records containing employee-specific information fall outside the scope of the *Act* and the jurisdiction of the IPC. Nevertheless, counsel informed the IPC that the affected employees were notified and given information on how to protect their identity information, as well as offers of credit monitoring services.

Scope of encryption

[62] Apart from exfiltration, the threat actor also deployed automatic ransomware encryption over the TSSO network's virtual infrastructure containing servers and disks. The custodians submitted that, although the precise assets encrypted were identified, an exhaustive investigation was not conducted to determine the specific individuals whose information was contained or the specifics of that information.

[63] For all hospitals, the encrypted servers included application servers that supported clinical care and diagnostic testing procedures and other servers with administrative functions. These locations contained personal health information of the hospitals' patients. For example, a server supporting an application related to point-of-care testing may have included information such as patient name, medical record number, and test result.

[64] For TDFHT, the encryption impacted Microsoft Exchange servers which the clinic relied on to use email hosting services. In addition, Microsoft software suite was encrypted, which did not contain personal health information.

[65] It was reported that the amount of the encrypted data, which included program and system files, exceeded 800 terabytes. While it is unclear what proportion constitutes the personal health information of patients, the overall scale of the encrypted data significantly overshadows the scale of data exfiltrated in this attack. There was limited overlap between exfiltration and encryption; the Scan Drive was automatically encrypted after it was exfiltrated, but the Shared Drive and the Database Report were not encrypted.

[66] The custodians informed the IPC that the threat actor deployed "container-level" encryption over the virtual infrastructure within the TSSO network. The custodians

[7] *See PHIPA,* s 4(3) (mixed records).

advised that, as a result, the threat actor did not view or exfiltrate information from these locations, with the exception of the Scan Drive which was exfiltrated before it was encrypted.

[67] I asked the custodians to provide their position on whether the hostile encryption in this case resulted in the theft, loss, or unauthorized use or disclosure of personal health information in the custody or control of the custodians. I further asked the custodians to state their position on whether the *Act* required them to notify the individuals whose personal health information was encrypted by the threat actor.

[68] The custodians submitted that the threat actor's encryption did not amount to any unauthorized use or disclosure, theft or loss of personal health information. Accordingly, the custodians took the position that they are not required under the *Act* to notify the individuals.

[69] Below, I will address the application of the section 12(2) notification requirement in this case and the custodians' position.

Issue 1: Does the notification requirement in section 12(2) of the *Act* apply in the circumstances?

[70] Under the *Act,* health information custodians have an obligation to notify affected individuals of a breach at the first reasonable opportunity. Section 12(2) states:

> (2) Subject to subsection (4) [not applicable in the circumstances of this matter] 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.
>
> [emphasis added]

[71] It is not in dispute that, for all six custodians, the threat actor exfiltrated personal health information which was a breach triggering the notification requirement under section 12(2).

[72] However, the custodians submitted that the threat actor's encryption did not result in the theft, loss, or unauthorized use or disclosure of personal health information and, therefore, they were not required to notify the individuals whose personal health

information was subject to the encryption. They argued that the encryption was automated and performed at the container level, such that no person reviewed or stole the personal health information within the encrypted containers.

PHIPA Decisions 253 and 254

[73] In PHIPA Decision 253, the IPC addressed the issue of whether container-level ransomware encryption triggered the duty to notify under section 12(2) of the *Act* (PHIPA Decision 254, issued concurrently, addresses similar issues pertaining to a different health information custodian). In that case, the ransomware attack resulted in the encryption of a hospital's virtual servers containing individuals' personal health information, and the hospital's position was that there was no evidence of exfiltration.

[74] In support of its position that it was not required to notify, the hospital in that case sought to distinguish between two types of ransomware encryption. In one type, threat actors may deploy ransomware (malware) onto specific files stored on computers or servers, resulting in the encryption of these files. In the other, threat actors can deploy ransomware at the "container" level, encrypting virtualized servers rather than the individual files stored within those servers.[8] The hospital argued that in the latter case, the threat actor could not view or access the contents of the encrypted container without decrypting the container.

[75] The adjudicator accepted the hospital's submission that the encryption did occur at the container-level, rather than at the level of individual files. She further accepted that the threat actor did not view or access any of the individual files of personal health information. However, the adjudicator found that the ransomware encryption was both "unauthorized use" and "loss" of personal health information within the meaning of section 12(2), and that the custodian was required to notify under that section.

[76] Section 2 of the *Act* states that "'use", in relation to personal health information in the custody or under the control of a health information custodian, means to view, handle or otherwise deal with the information, subject to subsection 6(1), but does not include disclosing the information. In the adjudicator's view, the container-level encryption, by transforming the external containers, also transformed the personal health information that was housed within, with the specific effect of rendering the information unavailable and inaccessible to authorized users of that information. She found that this effect constituted a use of the personal health information, because it involved a type of "handling" of or "dealing with" the information as contemplated in the definition of "use" under the *Act.*

[77] The adjudicator found that the custodian's maintenance of backups for the personal health information did not negate the fact that the information was rendered inaccessible by the encryption. Rather, the necessity of restoration by backups

[8] PHIPA Decision 253 at para 36.

highlighted the very effect of the encryption.[9] Furthermore, since the encryption occurred without the appropriate consent of the individuals and was not otherwise permitted or required to be done under the *Act,* the threat actor's encryption was found to constitute unauthorized use.[10]

[78] The adjudicator also found that the container-level encryption constituted a "loss" within the meaning of section 12(2). She observed that, regardless of whether the encryption occurred at the file level or at the container level, its effect of making unavailable the personal health information to the authorized user because of an unauthorized activity resulted in a loss of that information.[11]

[79] In finding that the encryption was both unauthorized use and loss of personal health information, the adjudicator noted the purpose behind the statutory duty to notify:

> 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.[12]

[80] Specifically, in the context of a ransomware attack, the adjudicator noted that a purposive definition of the terms "use" and "loss" in relation to the duty to notify, "contemplates notice to affected individuals where there has been an unauthorized action in respect of their personal health information."[13]

Custodians' submissions

[81] The submissions made by counsel in this case were substantively the same as those that were comprehensively addressed in PHIPA Decisions 253 and 254*.*

[82] Counsel argued that encryption did not result in the use of personal health information, since no person viewed or stole the information within the encrypted containers. He argued that PHIPA Decisions 253 and 254 were wrongly decided to the extent that they found that encryption without data theft and where the encrypted data were fully restored from backups results in "use" and "loss" of personal health information.

[83] For the hospitals, counsel advised that the encryption did however impact their patients' personal health information. The hospitals were prevented from accessing the information within the encrypted locations relating to clinical procedures such as point-of-care testing. Furthermore, BWH temporarily lost access to its own EMR containing patient data.

---

[9] *Ibid.* at para 41.
[10] *Ibid.* at para 43.
[11] *Ibid.* at para 50.
[12] *Ibid.* at para 53.
[13] PHIPA Decision 254 at para 38.

[84] From this information, it is evident that the ransomware encryption rendered the personal health information within the encrypted containers inaccessible to the hospitals and their authorized users.

[85] As for TDFHT, the hostile encryption affected the Microsoft software suite (including applications such as Microsoft Excel) and the Microsoft Exchange email server used by TDFHT staff. The counsel submitted that the encryption resulted in temporary operational and communication inefficiencies, but the clinic maintained access to the EMR which was not impacted by the attack.

[86] Regarding the email server specifically, counsel advised that since 2022, TDFHT exclusively uses a secure file transfer platform to share personal health information and has a policy not to share personal health information via email. However, prior to 2022, the clinic used email to share personal health information with patients when directed by patients or when it could not be communicated by phone. Furthermore, until 2023, certain records were forwarded to the clinic's receptionist using an efax software which allowed receipt of faxed documents by email.

[87] The clinic opted not to restore the contents of the email server from prior to the incident. However, counsel submitted that any personal health information which resided in the server was also available in the clinic's EMR. He argued that, therefore, losing access to emails in the server did not render inaccessible the personal health information.

[88] From the information provided, it appears that the email server housed personal health information of TDFHT's patients and that the hostile encryption denied TDFHT and authorized users access to that information within the server, resulting in a temporary loss of access, regardless of the clinic's decision not to restore that information on a go forward basis.

Analysis

[89] I accept the custodians' submission that the threat actor's encryption of the 192 servers on the TSSO network was deployed at the container level by targeting its virtual machine containers. I also accept the custodians' evidence in this case that the threat actor did not view or access the personal health information in the servers that have been encrypted.

[90] However, I do not agree with the custodians' characterization of the hostile encryption in terms of the *Act*. Rather, I agree with the reasoning in PHIPA Decisions 253[14] and 254 and choose to adopt the adjudicator's interpretation of section 12(2) in situations involving ransomware encryption.

[14] As of the date this decision was issued, PHIPA Decision 253 was still subject to an ongoing application for judicial review. Unless and until the court indicates otherwise, I find the adjudicator's reasoning in PHIPA Decision 253 to be reasonable, and I have adopted it in this decision.

[91] I find that in this case, the threat actor's encryption amounted to unauthorized use of personal health information in the custody or control of the custodians. The encryption of the containers and servers had the effect of transforming the personal health information contained therein, such that it was unavailable and inaccessible to authorized users of the information. Like the adjudicator in PHIPA Decisions 253 and 254, I find that this effect constituted a type of "handling" of or "dealing with" the information which meets the definition of use under the *Act,* specifically, by rendering inaccessible the personal health information to the custodians and authorized users.

[92] Furthermore, there is no suggestion that this use occurred with appropriate consent, nor that it was otherwise permitted by the *Act*. Therefore, I find, in the circumstances, that the threat actor's encryption constituted an unauthorized use of personal health information.

[93] It is evident that personal health information within the encrypted servers could no longer be accessed or used for authorized purposes. Because the encryption had this effect, I also find that the encryption constituted a loss of that information. To clarify, this loss of personal health information was the result of the hostile encryption, not the pervasive disruption of TSSO's services when it disconnected its network to contain the attack and prevent further harm.

[94] In my view, the availability of backups does not preclude the above findings. Again, in PHIPA Decision 253, the adjudicator noted:

> … 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.[15]

[95] Maintenance of backups remains an integral part of secure information practices and vital to system recovery and mitigation of service disruption. However, the fact that the same information exists in backups does not negate the fact that the custodians could no longer retrieve or use the information in its original digital location. The same principle applies where the duplicate information exists in other locations not impacted by encryption, such as the EMR in the case of TDFHT.

[96] Not recognizing the encryption event as a loss would imply that individuals would be left uninformed of the incident in which a malicious third-party compromised the custodians' control over personal health information and the security of the systems to which the individuals entrusted their information. In my view, this result would not be

[15] PHIPA Decision 253 at para 49.

consistent with the purpose of the duty to notify and run contrary to the obligation of custodians to ensure the security of personal health information.[16]

[97] As alluded to in PHIPA Decision 253, the statutory duty to notify underscores the fundamental understanding that personal health information "belongs" to the individuals to whom it relates and that they are entitled to know what happens to it in the custody or control of custodians to whom the information is entrusted, particularly where malicious actors are involved.

[98] Counsel for the custodians submitted that requiring the custodians to notify would have negative implications, noting that in PHIPA Decision 253, the adjudicator acknowledged the risk of "notification fatigue on the part of the public, disproportionate costs to the custodian, and other unintended and undesirable consequences" when requiring notification in certain circumstances.[17]

[99] I disagree with this interpretation. In PHIPA Decision 253, the adjudicator was considering the potential harms associated with notification if an overly broad interpretation of "loss" were used. The adjudicator was referring to certain scenarios, such as routine maintenance or an unexpected power outage which, notwithstanding that the custodian is temporarily unable to access personal health information, may not necessarily be interpreted as "loss". The adjudicator distinguished these situations from instances of encryption by a malicious actor, which she found was a "loss" of information that warranted notification.

[100] Furthermore, such harms can be mitigated by selecting an appropriate method of notification. For instance, while direct written notice to each affected individual may be the appropriate method of notification in many cases, the IPC has also accepted indirect written notice to the public as an appropriate alternative where the direct notice would not be feasible or practical.[18]

[101] For the above reasons, I find that the threat actor's ransomware encryption of TSSO's virtual infrastructure constituted both unauthorized use and loss of personal health information of patients of the custodians. Accordingly, I find that the custodians were required under section 12(2) to notify the individuals affected not only by the data exfiltration but also by the hostile encryption.

Issue 2: If the notification requirement applies, was notice given in compliance with section 12(2)?

[102] When evaluating compliance with the notice requirement, the IPC has considered principles outlined in its guidance document *Responding to a Health Privacy Breach:*

---

[16] *PHIPA,* s 12(1).
[17] PHIPA Decision 253 at para 51.
[18] PHIPA Decision 210 at paras 27-28.

Guidelines for the Health Sector.[19] The IPC acknowledges that the best form of notification in each case will depend on many factors.

[103] It is expected that notification will include information such as the date of the breach, the description of the nature and scope of the breach, the description of the personal health information that was impacted, and the measures implemented to contain and remediate the incident. The notice must also include a statement that the individual is entitled to make a complaint to the IPC. Of course, a custodian is not expected to have completed its entire breach investigation at the time notification occurs (which must be at the first reasonable opportunity).

[104] TDFHT issued a direct notice letter to every patient on record during the week of January 8, 2024.

[105] The notice includes a description of the incident, a description of the types of personal health information that was exfiltrated, and the steps that were taken and will be taken to contain and address the incident. The notice describes that the incident was "a ransomware attack involving the theft of some data from servers maintained by [TSSO]" and that the threat actor stole data stored on a shared drive.

[106] The notice provides the clinic's contact information in case of any questions. It also notes that while the recipient is entitled to file a complaint with the IPC, it is not necessary as the IPC is already investigating the matter.

[107] In addition to the direct notice, TDFHT also published an indirect notice on its website. While the initial date of publication is not known, TDFHT submitted that in May 2024, the indirect notice was revised to replicate the full content of the direct notice.

[108] The direct notice was issued approximately two months after the incident. However, during that period, the clinic consulted with the IPC regarding notification. Given the above, I find that TDFHT notified the affected patients at the first reasonable opportunity.

[109] Overall, I am satisfied that the clinic notified the patients affected by the exfiltration of personal health information consistent with section 12(2).

[110] However, the notice does not acknowledge that hostile encryption occurred and does not provide any related facts. It does not describe the personal health information stored in the encrypted email server, nor the encryption's impact on the clinic's ability to retrieve the information from that server.

[111] Therefore, I find that, in respect of the hostile encryption, TDFHT did not notify the affected individuals in compliance with section 12(2) of the *Act.*

[19] For example, *see* PHIPA Decision 266 at para 69.

[112] As for the hospitals, between October and December 2023, they and TSSO published media releases regarding the incident on their respective websites. These releases provided coordinated updates on the ongoing investigation and findings, such as the types of patient and staff information exfiltrated by the threat actor and the number of individuals affected as a result.

[113] In April 2024, following consultations with the IPC, the hospitals published a further release entitled "public notification". This notice provides the number of patients whose information was stolen for each respective hospital and states that they will be receiving notice letters. It also directs the reader to a published Frequently Asked Questions document regarding the cyberattack and the hospitals' incident response.

[114] The IPC received templates of the direct notice letters issued to individual patients in April 2024. They include a description of the incident, the scope of personal health information that may have been exfiltrated, and steps that were taken or will be taken to contain and remediate the incident. For patients whose SINs were compromised, the letters also include offers of credit monitoring services.

[115] The notices provide contact information for any questions, and state that while the recipient may file a complaint, the IPC is already investigating the matter.

[116] While I acknowledge the wide campaign which the hospitals undertook to inform the public regarding the incident, it is apparent that both the direct notices and the public releases focused exclusively on the threat actor's *exfiltration* of personal health information, without acknowledging the hostile *encryption* and its significance. They do not acknowledge the hostile encryption event or provide related details. Some public releases make reference to the fact that a ransomware attack occurred and to technical issues experienced at the time of the incident. However, I am not satisfied that this information sufficiently provides notice of the hostile encryption and its impact.

[117] Based on the above reasons, I find that the hospitals did not notify the affected individuals in compliance with section 12(2) of the *Act.*

[118] Counsel argued that if they were required to notify of the hostile encryption event, such notice would be confusing and vague. They provided the following hypothetical language of notification as an example:

> We were subject to a ransomware attack. It was not a data breach. The virtual storage container holding the data containing your PHI was encrypted, temporarily restricting access to your PHI for a short period of time. All data was backed up, restored, and it is now fully available. Your PHI was not read or reviewed. It was not copied. It was not deleted. It was not stolen or given away. No unauthorized person has your information. You are not at risk of identity theft or harassment from this incident.

[119] In my view, this hypothetical example of notification is misleading because it

misrepresents what would be required to be included in a notice. It lacks details that would meaningfully inform the reader about the encryption and its significance. For instance, it does not describe the encryption's immediate impact on the custodian's ability to access the information. Further, the contents of a required notice would give information about the steps the custodian is taking to contain and remediate the breach, including restoration of the information from backups. A proper notice that contains a concise and accurate description of the breach and the custodian's response to it would not be vague or confusing.

[120] Further, counsel for the custodians submitted that requiring notification about encryption would cause the custodians significant administrative burden as well as notification fatigue to recipients.

[121] As alluded to above, appropriate notification can take many forms. This may have been an instance in which indirect notification in the form of public notices would be appropriate. For example, it was open for the custodians to seek the IPC's guidance on including, in their public releases, information about both the data exfiltration and the hostile encryption. This approach could have served to fulfill the requirement at once, avoiding the need for redundant notification, and thereby mitigating concerns of administrative burden and notification fatigue. Furthermore, the public would have been provided with a more transparent and comprehensive account of the incident. Lastly, it is difficult to see how a simple indirect notification would significantly increase the administrative burden. Regardless of whether notification is required or not, the custodian is still required to contain, investigate, and remediate the breach.

[122] While I find that the custodians did not notify as required, I note that they have been identified in this decision and that their patients, now informed of the hostile encryption, are able to contact them for more information. Based on this fact and other circumstances of this case, including the passage of time since the incident, the notification already completed to date and public communications made regarding the incident, I find that there is no useful purpose in ordering the custodians to issue additional notification at this stage.

Issue 3: Did the custodians take reasonable steps to protect personal health information?

[123] Section 12(1) of the *Act* requires health information custodians to take reasonable steps to protect the security of personal health information in their custody or control. This requirement includes a duty to respond promptly and adequately to a privacy breach. In addition to notification (discussed above), a proper breach response helps ensure that the privacy breach is immediately contained, an investigation is carried out to determine the root cause of the breach and appropriate remedial steps are taken to mitigate the

risk of reoccurrence.[20]

[124] A related obligation is the duty to have in place and to comply with information practices, including administrative, technical and physical safeguards and practices with respect to personal health information in their custody or control [sections 10(1) and 10(2)].[21]

[125] In their responses to the IPC, the custodians provided details of the steps taken by their agent TSSO, whose network was targeted by the threat actor and was primarily in charge of responding to and investigating the cyberattack on behalf of the custodians.

[126] The custodians also provided the IPC with two incident response protocol documents developed and maintained by TSSO on behalf of the custodians, which I find helpful in analyzing the adequacy of their breach response measures, particularly in the event of a cyberattack. Below, I provide a brief overview of each document.

TSSO IT Incident Management Playbook

[127] TSSO IT Incident Management Playbook (the Playbook) governs how TSSO will respond to and recover from major IT incidents including, but not limited to, cyberattacks.

[128] It notes that there are many possible causes for major IT incidents/outages/downtimes and that the plans outlined would be enacted in the event of a major IT systems outage regardless of the cause of the outage. It notes that "[i]n the event of a major, high severity IT systems issue, [TSSO] must be able to respond quickly, continue to support its member hospitals and recover services as soon as possible."

[129] The Playbook breaks down TSSO's incident management protocol into three main components: incident response, business continuity plans, and incident recovery plan. For each component, the Playbook outlines concrete tasks and processes that should be prioritized in the event of a major IT incident. The document specifies the relevant purposes of these tasks, the processes, and the staff and stakeholders who will be responsible for executing them.

[130] According to the Playbook, the overall incident response plan is comprised of the initial incident identification, followed by a set of high-level tasks designed to determine the incident's severity, size, scope and impact. Once assessment is completed, TSSO follows agreed protocols for communicating the incident both internally at various levels of TSSO and externally to member hospitals. The document notes that alternative communication methods are considered to account for potential impacts of system outages.

---

[20] PHIPA Decision 253 at para 14.
[21] PHIPA Decision 110 at para 64.

[131] The incident response plan considers possible scenarios of system outages and outlines priority steps to address impacts on critical clinical systems and specific applications. In the event of a ransomware attack, TSSO will engage a third-party cyber security company to provide onsite support and assume leadership in the incident response. The response will include support from consultants and industry experts to provide guidance on best practices regarding the response, negotiations and recovery from the attack.

[132] The second section relates to business continuity plans for maintaining critical processes, particularly in the event of increased downtime. These processes contemplate necessary alternative protocols, staffing adjustments, resources and technologies, based on identified short-term and long-term continuity plans for each department.

[133] The third section relates to incident recovery. The Playbook establishes a general priority list for the restoration of TSSO's IT services and provides that an incident recovery should begin by identifying the relevant tasks required for the recovery of clinical systems, business systems and end point devices. Notably, the plan acknowledges that recovery efforts should consider factors such as the magnitude of the incident, the length of the incident and impacts to data and back-ups if any. It also notes that recovery of patient-facing critical clinical systems must be prioritized.

TSSO Ransomware Response Procedure

[134] TSSO maintains a separate document for its response procedure specifically to ransomware attack incidents (the Ransomware Response Procedure).

[135] The stated purpose of the Ransomware Response Procedure is to "define the procedures by which [TSSO] will respond to a significant Ransomware Cyber Security event related to [TSSO] managed systems". The document identifies specific roles and responsibilities of stakeholders who will participate in the incident response. It then establishes the following phases a standard incident response lifecycle: preparation detection, containment, investigation, remediation, and post-incident (recovery).[22]

[136] For each of these phases, the document identifies priority tasks, their objectives and the teams that will be responsible for those tasks.

[137] I note that the document does not explicitly define the activities of evidence collection. I asked the custodians about the absence of detailed evidence gathering activities in the Ransomware Incident Response Procedure. The custodians submitted that TSSO took the following steps to preserve evidence at the containment stage:

[22] The document refers to National Institute of Standards and Technology (NIST) publication SP 800-61 (Computer Security Incident Handling Guide) where these phases are defined.

- Isolate servers and prevent further access or modification until breach counsel and forensic investigators were engaged;
- Prevent access to physical facilities until the forensic teams arrived; and
- Sever all remote access and internal access to secure the servers and prevent spread of malicious of software or exfiltration of data, ensuring data integrity and preserving evidence for forensic collection.

[138] I acknowledge that these are important and appropriate steps which facilitated later forensic investigation to determine the nature and scope of the attack. However, clearly defining evidence collection activities in advance can assist in early detection and containment of an ongoing attack and ensure consistent response in the future. For this reason, I recommend that the custodians work with TSSO to ensure that the Ransomware Response Procedure proactively sets out clearer evidence collection activities, including the types of sources from which evidence could be obtained.

[139] With that caveat, I find that overall, the Playbook, combined with the Ransomware Response Procedure, provide a comprehensive incident response framework in the event of a ransomware attack incident. I will now go on to assess the adequacy of the custodians' response in this case, including their containment, investigation and remediation measures.

Containment

[140] Upon discovering the threat actor's ransomware note, TSSO engaged its incident response plan and executive escalation protocols. TSSO disconnected its systems from VPN access, and severed and/or reconfigured various internal and external access points. In addition, all local administrator access accounts were removed and all user accounts were locked out.

[141] According to the custodians, these steps stopped the shell script that was deployed by the threat actor to execute malicious commands in the TSSO environment, preventing further compromise of data.

[142] TSSO dedicated additional staffing to provide enhanced cybersecurity monitoring and increased monitoring of activities passing through the firewall.

[143] Furthermore, TSSO implemented dark web monitoring. It was discontinued shortly after the threat actor published the exfiltrated data. However, several months after the incident, the custodians advised the IPC that it had resumed monitoring. Further to my recommendation based on recent precedents, the custodians agreed to continue with dark web monitoring for two years from the date of this decision.[23]

---

[23] PHIPA Decision 210 at para 21; *see also Re Nova Scotia Health Authority*, 2020 NSOIPC 2.

[144] TSSO securely erased and reformatted the encrypted servers, recognizing that without completely wiping and reformatting these servers, a risk of corruption or potential reattack would have remained. The custodians advised that reformatting these servers before restoring them using backups would preclude any access by the threat actor.

[145] As for the servers which were exfiltrated but not encrypted, these were isolated allowing for security scanning and confirmation of patching before they were returned to service.

[146] Overall, I find that the custodians implemented adequate measures to contain the breach after the ransomware attack was discovered. The decision to disconnect the TSSO network, while causing significant disruption of the custodians' operations, was appropriate in the circumstances to mitigate the impact of the ongoing attack and prevent further infiltration and compromise of personal health information.

[147] It was reported that it took approximately five hours between the time network issues were first reported and the time the network was disconnected. This was due in part to initial symptoms of technical malfunction presenting as low severity, until failing remote logins prompted urgent troubleshooting which began within one hour. The custodians submitted that TSSO's initial troubleshooting steps, once triggered, were reasonable to ensure timely detection and analysis.

[148] I find that the overall response time was reasonable in the circumstances. However, I note that over two hours elapsed between the time when slow response rates and difficulty logging into applications were first reported (initially considered a low severity issue) and the time when remote logins began failing altogether, prompting an urgent response as a high severity issue. TSSO's Ransomware Response Procedure documentation, discussed above, describes staff responsibilities in incident detection, such as asking investigative questions and identifying signs of suspicious activities. However, the documentation does not provide details of how alerts should be classified or the estimated response time. From the information provided, it is unclear whether the initial network issues could have been classified and assessed differently, so as to enable a prompter analysis of the systems before the issues evolved to high severity status.

[149] I recommend that the custodians work with their agent TSSO to review their early detection process, ensuring that an incident alert is classified properly and that the initial assessment of the alert is effective.

Investigation

[150] After TSSO disconnected its network, it was left on standby until law enforcement and TSSO's forensic teams were contacted. Until their arrival, TSSO secured the physical facilities, and the encrypted servers were left running.

[151] The forensic teams examined the affected systems to understand the extent of the breach. They gathered information and performed system memory checks to

determine if there were any persistent security threats. Available system and network logs were analyzed to trace the threat actor's activities.

[152] Other methods used to investigate included review of various system logs and browser history, antivirus scanning, and the download and inspection of the exfiltrated files and the file lists published by the threat actor.

[153] To determine the types of personal health information exfiltrated and the individuals affected, a third-party data mining vendor was engaged.

[154] As part of my investigation, I inquired about the three administrator accounts that the threat actor used to infiltrate the attack, specifically, how these accounts came to be compromised in the first place. The custodians submitted that the forensic investigation was unable to determine how the accounts came to be compromised.

[155] The exposure of the accounts' credentials played a pivotal role in allowing the threat actor to exfiltrate and encrypt large amounts of data including personal health information.

[156] An indispensable part of an investigation following a cyberattack incident is determining the root cause of the attack. There may be more than one root cause, depending on the sophistication of the information infrastructure involved. Generally, to successfully remediate a breach and mitigate the risk of recurrence, root cause vulnerabilities must be identified and addressed.

[157] It is possible that despite adequate forensic investigation, a custodian will not be able to identify the root cause of a cyber incident. However, it is incumbent upon the custodian to demonstrate that they have conducted a reasonable investigation into the circumstances.

[158] In the present case, counsel advised that TSSO's forensic investigation was unable to determine how the three accounts used in the attack were initially compromised. He submitted that this was because pertinent evidence residing on encrypted systems was lost, since hospitals decided not to pay a ransom in exchange for the threat actor's decryption key.

[159] I do not find particularly compelling their submission that pertinent evidence of account compromise resided on encrypted systems. The threat actor initially entered the TSSO environment by leveraging one account which had already been compromised. It appears unlikely that the evidence of this compromise would be found in the very systems which the account was used to infiltrate. While theoretically, the threat actor could have obtained the credentials of two other accounts after successfully entering the network, I have not received further information which would suggest this possibility or that the evidence of account compromise would have otherwise existed in the encrypted systems.

[160] Counsel submitted that although the root cause of the compromise could not be

determined, the forensic investigation still explored all available evidence and investigative avenues. The forensic tools and methodologies used to investigate involved various techniques such as data imaging, penetration testing and reverse engineering.

[161] The investigation also included consultation with the original holders of these accounts, a TSSO staff member, and BWH's third-party vendor. The account holder from TSSO did not report of any phishing, suspicious emails, or suspected credential loss or theft. As for the vendor, its support team confirmed that they had no reports of any internal compromise.

[162] Furthermore, TSSO arranged third-party forensic analysis of the staff member's machines. However, no indicators of compromise or phishing emails were found.

[163] Although the root cause vulnerabilities behind the compromise of the three administrator accounts could not be determined, TSSO implemented an array of measures that would prevent a similar attack.

[164] The administrator accounts were disabled and later redeployed where applicable following a password reset. The account that was used to establish initial connection to the TSSO network had its remote access capability disabled. Also, the accounts are now managed using a privileged access management solution.

[165] Specifically, MFA was enabled for the two of the three accounts. The third account, used by BWH's third-party vendor, could not be configured with MFA due to a technical limitation. However, in response to the incident, BWH migrated its EMR system to a remote solution outside the TSSO network, thus limiting future reliance on the vendor account. BWH will continue to utilize this vendor for other administrative functions until BWH can transition to a new system. Furthermore, TSSO implemented a special process whereby the vendor access will be controlled manually with enhanced monitoring for any suspicious activity.

[166] From the available facts, it appears that the lack of MFA for the three administrator accounts was a likely contributing factor in how their credentials came to be compromised in the first place. Nevertheless, overall, I am satisfied that TSSO conducted an adequate investigation into the compromise of the three administrator accounts that the threat actor used to infiltrate the TSSO network. In addition, I am satisfied that, although the root cause behind the compromise could not be determined, TSSO adequately identified and addressed the relevant gaps and vulnerabilities in its systems.

Remediation

[167] Even where the root cause vulnerabilities could not be determined, it remains the responsibility of the custodian to take reasonable remedial actions that address possible avenues of a similar attack.

[168] According to the custodians, TSSO undertook a significant mitigation and

hardening effort to reinforce the cybersecurity of its systems. Remedial measures were taken to address different layers of risk exposure.

[169] To mitigate risk factors associated with large data movements, TSSO put in place additional access restrictions and safeguards. For instance, external traffic flow was restricted based on recognized and approved destinations. TSSO increased scanning and monitoring of traffic and deployed reinforced firewalls and detection systems.

[170] Additional safeguards were deployed to improve detection of compromised account credentials or suspicious activities and limit a potential threat actor's ability to download and install tools which would facilitate exfiltration of data. In addition, TSSO will be implementing file integrity monitoring by early 2026 to help detect malicious access and alteration of system files.

[171] Since file integrity monitoring will not be implemented until 2026, I recommend that the custodians work with TSSO to ensure that appropriate measures are implemented to ensure that related risks are adequately evaluated and managed in the interim period.

[172] To mitigate exposure risk associated with user accounts, TSSO forced a password change supported by individual staff verification and reset its password authentication solutions. MFA was deployed for all user accounts. Network access for vendors was also reinforced with MFA or approved secure access methods. As for administrator accounts, remote access was disabled and MFA deployed where applicable.

[173] Specifically in relation to BWH, TSSO relocated BWH-specific network assets from BWH's local computer room to TSSO's data centre for increased security. In addition, BWH transitioned its EMR system from its existing third-party vendor to a remotely hosted solution, therefore limiting future exposure risk associated with a vendor-controlled administrator account. Other restrictions were implemented to prevent access to other hospital assets and any internet access to and from the network.

[174] TSSO also performed penetration testing of all exposed systems and applications.

[175] In my investigation, I inquired whether the custodians conducted a threat and risk assessment (TRA) following the system recovery. Counsel advised that BWH has completed its TRA in October 2024 while other hospitals and the clinic will be completing separate TRAs after securing a suitable third-party provider. The custodians have committed to completing the TRAs by September 2025.

[176] TRAs are an important part of maintaining an organization's cybersecurity framework, particularly following recovery from a privacy breach. [24] In the present case,

[24] As reference, the National Institute of Standards and Technology provides guidance on conducting risk assessments as part of an organization's cybersecurity management program; *see* "SP 800-30, Revision 1,

as discussed further below, the custodians could not identify the exact root cause of the breach. In such circumstances, it is particularly important to identify the potential threats and vulnerabilities through a formal TRA and ensure that the remedial measures taken adequately address those risk factors.

Incident recovery

[177] The custodians submitted that, upon completing the forensic work, TSSO began restoration of the services that were disrupted following the ransomware encryption and subsequent network shutdown.

[178] TSSO reconstructed a new, secure environment into which it restored viable backups, on the advice of third-party security consultants. The environment was rescanned for vulnerabilities and virus/malware activity.

[179] TSSO utilized backup solutions which included procedures to enhance security and integrity of the data, such as ensuring that backup copies are safely isolated from original data and are protected from alteration or deletion, and robust data access controls. At the time of the ransomware attack, the backup systems were unconnected to the network and were not affected by the incident.

[180] The core clinical services for the hospitals, such as the EMR, lab systems and communication systems, were fully restored within several months following the incident. Other systems were prioritized for restoration over 2024 and 2025. Restoration of all services for TDFHT including IT infrastructure was completed by January 2024.

TSSO privacy and security training

[181] Where the third-party service provider falls victim to an attack, the custodians should ensure that remediation includes review and, if necessary, improvement of the provider's training policies and practices on privacy and security.

[182] The custodians submitted that TSSO staff receives privacy and cybersecurity training upon hiring and annually thereafter. I reviewed TSSO's "ISS 002" Information Security Training policy document. It mandates privacy and security training for all employees and contractors and specifically notes that the training objectives include:

- Explaining TSSO's obligations under the *Act;*
- Describing how TSSO plans to achieve its privacy and security objectives and organizational goals;

Guide for Conducting Risk Assessments" (https://csrc.nist.gov/pubs/sp/800/30/r1/final) and "SP 800-61, Revision 2, Computer Security Incident Handling Guide" (https://csrc.nist.gov/pubs/sp/800/61/r2/final).

- Clarifying practices TSSO staff should follow to achieve compliance with the *Act*; and

- Increasing awareness of the necessity to safeguard TSSO's corporate information and its members' or clients' personal information and personal health information.

[183] The policy requires the training to be reviewed and refreshed annually and employees and contractors recertified.

[184] I also reviewed the TSSO's privacy and security training materials provided by the custodians, including a presentation for TSSO staff, consultants and management, as well as employee onboarding quiz questions.

[185] The training materials provide guidance on TSSO's obligations under the *Act* and its privacy objectives and practices to achieve compliance with the legislation. In addition, they explain privacy principles such as accountability, consent and safeguarding from unauthorized activities and misuse. They also provide other useful practical guidelines on identifying suspicious activities and secure information handling practices. For example, employees are educated on identifying email fraud, which can take the form of direct threats, spoofing of popular websites, or phishing emails that appear as legitimate correspondence.

[186] TSSO also provides ongoing security-awareness and training to its staff related to protocols associated with administrator accounts. For example, TSSO maintains a security and approval process that outlines those within TSSO and the hospitals who require administrator access and validating their identities before granting administrator access. The protocols also include administrator account monitoring and access logging.

[187] Based on the information provided, I am overall satisfied that TSSO as the custodians' agent maintains adequate training policies and practices related to cyber security and privacy.

Relationship between the custodians and TSSO

[188] During my investigation, I asked the custodians about their relationship with TSSO and any related agreements.

<u>The hospitals</u>

[189] The hospitals founded TSSO as a not-for-profit organization. As founding members, the hospitals participate in TSSO's governance by providing their executives as directors to TSSO's board of directors. The hospitals also provide funding to TSSO's overall budget.

[190] The hospitals provided the IPC with a copy of their service agreement with TSSO. The agreement is comprehensive and detailed, setting out the IT services to be provided

by TSSO. It states that the agreement is intended in good faith to meet the requirements of the *Act* that address the protection of personal health information, and that TSSO acts as an agent for the hospitals as defined in the *Act* when performing services under the agreement.

[191] The agreement contains express provisions governing the security, confidentiality and privacy of data. For instance, it acknowledges the hospitals' continued ownership of the data provided to TSSO including personal health information, and limits TSSO's access to and use of the data to the purposes of providing its services. In addition, TSSO is required to implement security safeguards, demonstrate compliance with its data handling obligations by way of privacy impact assessments and audits, and ensure proper staff training.

[192] Overall, I am satisfied that the provisions found in the hospitals' agreement with TSSO are in keeping with the hospitals' privacy and security obligations under the *Act,* including section 12(1) of the *Act.*

TDFHT

[193] The IPC also received a copy of the service agreement between TSSO and TDFHT. The agreement clearly outlines the scope of TSSO's IT services and its technical support obligations. In addition, it provides TSSO's commitment to "demonstrate care to maintain and make every reasonable attempt to protect personal health information". It contains certain standard provisions, such as those related to subcontracting of services and compelled disclosure, and limits on the use and disclosure of confidential information, which is broadly defined.

[194] However, the agreement otherwise lacks key provisions related to privacy, confidentiality and security of the data that would support the clinic's compliance with the privacy and security requirements of the *Act*.

[195] For instance, the agreement does not establish whether the clinic maintains continued ownership and control of personal health information that is provided to TSSO. The agreement does not expressly set limits on TSSO's collection, use and disclosure of personal health information, and is silent on training requirements for TSSO staff. Importantly, the agreement does not require TSSO to comply with the *Act* and does not implement means by which TSSO can demonstrate its compliance.

[196] Retention of third-party services, especially IT services related to the storage and management of personal health information, is a common and integral part of modern health care services. A custodian may permit an agent, such as its third-party service provider, to collect, use or disclose personal health information on its behalf. However, the custodian retains responsibility for the information that is provided to the agent.[25]

[25] *PHIPA,* s 17.

[197] As such, when a custodian retains a third-party service provider to store and manage personal health information on its behalf, the custodian must take all reasonable and appropriate measures to ensure that the service provider deals with the entrusted information in a manner which complies with the custodian's obligations under the *Act.* An important means of achieving this objective is the implementation of enforceable contractual provisions which ensure that the third party's data handling practices comply with the privacy and security obligations under the *Act.*

[198] In Privacy Investigation Report PC12-39, *Reviewing the Licensing Automation System of the Ministry of Natural Resources, A Special Investigation Report* (MNR Report), the IPC identified key contractual provisions that help to mitigate the likelihood of a breach where private sector entities are engaged to handle records of personal information.

[199] More recently, the IPC recently issued its guidance document "*Privacy and Access in Public Sector Contracting with Third Party Service Providers*", which outlines best practices for public sector institutions for exercising due diligence and ensuring accountability when retaining third-party services. The guidance includes principles for determining how service providers can collect, use and disclose personal information, as well as contractual provisions, based on previous reports of the IPC, for ensuring that all reasonable steps are taken to protect the privacy and security of personal information.

[200] In my view, the outlined principles and contractual provisions referred to above are also relevant and instructive to health information custodians, who must take all reasonable steps to ensure that personal health information is protected against theft, loss or unauthorized use or disclosure.

[201] During my investigation of this matter, I referred the clinic to MNR Report and the types of contractual provisions that would help mitigate the risk of a privacy breach associated with third-party service providers, recommending that the clinic amend its agreement accordingly. The clinic has confirmed that its agreement has been revised in accordance with the IPC's guidance.

[202] Given the above, I am satisfied that the custodians have put in place appropriate contractual safeguards in keeping with section 12(1) of the *Act.*

Bluewater Health's collection of social insurance numbers

[203] As noted previously, the exfiltrated data included SINs of approximately 20,000 patients of BWH. When asked why BWH was required to collect SINs, counsel advised that it was to enable Workers Compensation Board's, and later WSIB's, record management protocols which used SINs as unique identifiers for record acquisition purposes during communications, billing, and other administrative activities. No further information was received regarding this requirement, other than that it came to BWH's attention that the collection was no longer required. Counsel also confirmed that BWH

was not authorized by any statute to collect SINs from patients seeking treatment related to WSIB claims.

[204] The exfiltrated SINs also included those collected between 1999 and 2006 from patients not involved with WSIB. BWH was unable to determine why the SINs were collected and why this practice ceased in 2006.

[205] In my view, the collection of patients' SINs by BWH created a point of vulnerability which in this case contributed to the severity of the privacy breach, exposing patients to added risk of threats such as identity theft and financial scams. I am not satisfied that the hospital has established that it had authority under the *Act* for the collection and retention of this information. Specifically, I am not convinced that BWH's collection of patients' SINs was in accordance with the data minimization principle in section 30 of the *Act.*

[206] Section 30(2) generally requires that health information custodians not collect more personal health information than is reasonably necessary to meet the purpose of the collection. While section 30(3) provides an exception where collection of personal health information is required by law, BWH in this case did not provide a basis in law for collecting the patients' SINs.

[207] Despite these concerns, the hospital ceased collection of SINs effective May 2024 and has confirmed that all collected SINs have been purged from BWH's records. Furthermore, the affected patients were notified and were offered credit monitoring services to help mitigate the risk of further harm.

[208] Accordingly, I am satisfied that BWH has appropriately addressed this matter in response to the incident.

CONCLUSION:

[209] The privacy breach in this case demonstrates the importance of custodians ensuring that they have in place adequate safeguards against cybersecurity threats when employing third-party information infrastructure and services.

[210] The lack of privileged account management processes for the administrator accounts used by the threat actor, including MFA, was likely a contributing factor in how their credentials were compromised in the first place. Although TSSO had measures in place to monitor traffic and limit the risk of infiltration, the threat actor was able to avoid early detection using these legitimate accounts.

[211] Following the incident, TSSO identified and addressed gaps in consultation with its security experts, by increasing monitoring and restricting of Internet traffic in and out of the network; deploying MFA to administrator accounts and disabling their remote access capability; and limiting exposure associated with vendor access through the migration of

services and more stringent access controls.

[212] In addition, TSSO undertook measures to improve its incident response, for instance, by conducting external review and audits of the incident response, adjusting policies and procedures – such as the chain of command that is activated upon breach – with the support of third-party experts, and launching working groups to generate further recommendations for improvement.

[213] I also note that TSSO and the hospitals have recently implemented improved privacy and cybersecurity policies and are in the process of adopting additional policies in other areas such as data storage and internal sharing, cybersecurity and privacy training, data governance, data backup and recovery, to be completed by mid-2025.

[214] Based on my analysis above, I make the following findings and recommendations.

[215] The threat actor exfiltrated from the TSSO network records containing personal health information of the custodians' patients. This exfiltration constituted unauthorized use and disclosure of the personal health information which triggered the custodians' duty under section 12(2) to notify the affected patients.

[216] I also find that the threat actor's encryption of network assets, which rendered inaccessible personal health information of patients of the custodians, was an unauthorized use and loss of the information for which the custodians were also required to notify under section 12(2).

[217] I find that the custodians appropriately notified the individuals who were affected by the exfiltration of their personal health information. However, the custodians did not notify affected individuals regarding the ransomware encryption and its impact on the patients' personal health information, which they were required to do. Therefore, I find that the custodians did not notify in compliance with section 12(2) of the *Act.*

[218] After reviewing the details of the incident, investigation and the information infrastructure involved, I am satisfied that the custodians have put in place appropriate measures to contain and remediate the incident and to ensure reasonable safeguards.

[219] Nonetheless, I have made recommendations for the custodians to further improve their practices. Namely, I recommended that the custodians:

- review TSSO's early detection process, ensuring that an incident alert is classified properly and that the initial assessment of the alert is effective;
- review TSSO's Ransomware Response Procedure to ensure that it establishes how alerts are classified and estimated response time;
- review TSSO's Ransomware Response Procedure to ensure that it proactively sets out clearer evidence collection activities, including the types of sources from which

evidence could be obtained; and

- ensure, pending TSSO's anticipated implementation of file integrity monitoring, that related risks are adequately evaluated and managed in the interim period.

NO REVIEW:

Section 58(1) of the *Act* sets out the Commissioner's discretionary authority to conduct a review as follows:

> The Commissioner may, on his or her own initiative, conduct a review of any matter if the Commissioner has reasonable grounds to believe that a person has contravened or is about to contravene a provision of this Act or its regulations and that the subject-matter of the review relates to the contravention.
>
> In accordance with my delegated authority to determine whether to conduct a review under section 58(1) of the *Act,* and based on the remediation steps already taken and the custodians' commitments to make further improvements, I conclude that pursuing a formal review under Part VI of the *Act* is not warranted.

Original Signed by: June 16, 2025

Francisco Woo
Investigator