Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

August 9, 2024

**VIA EMAIL**

**PERSONAL AND CONFIDENTIAL**

Travis Walker
Senior Associate
Norton Rose Fulbright Canada LLP
222 Bay Street
Suite 3000, P.O. Box 53
Toronto, ON M5K 1E7

Dear Travis Walker:

**RE: Reported Breach HR23-00282**

On June 5, 2023, you reported a breach of the *Personal Health Information Protection Act* (the *Act* or *PHIPA*) on behalf of a prescribed person under *PHIPA* to the Office of the Information and Privacy Commissioner of Ontario (IPC). File HR23-00282 was opened by the IPC to address this matter.

The circumstances of the breach involved the unauthorized copying of approximately 3.4 million individuals' personal health information (PHI) from the prescribed person's secure file transfer server. The threat actors gained unauthorized access to the server by exploiting a zero-day vulnerability[1] in the file transfer software, MOVEit, that was installed on this server.

## I. Background

### *What is a "prescribed person" under PHIPA?*

Prescribed persons under *PHIPA* compile or maintain registries of personal health information to enable or improve the provision of health care. Prescribed persons under *PHIPA* are identified in section 13(1) of Ontario Regulation 329/04 – General. Prescribed persons generally compile registries about a specific condition or disease.

The prescribed person that was subject to the cyberattack at issue in this breach is Ontario's prescribed perinatal, newborn, and child registry with the role of facilitating quality of care for families across the province.

[1] A zero-day vulnerability is a software vulnerability that is not yet known by the vendor, and therefore has not been mitigated. A zero-day exploit is an attack directed at a zero-day vulnerability. See Glossary - Canadian Centre for Cyber Security.

This prescribed person collects, uses, and discloses information about pregnancy, birth, the newborn period, and childhood to help improve care in compliance with section 39(1) of *PHIPA*. The prescribed person collects data from healthcare providers, labs, and hospitals, among other data contributors, who offer fertility, pregnancy and child health care, and processes this data before packaging it into information that healthcare providers and organizations can use to guide care and improve decision making.[2] The prescribed person's data collection, use, and disclosure is approved by law, regulated by the IPC, and funded by the Ontario Ministry of Health.

***What Happened?***

On May 31, 2023, the prescribed person was impacted by a cybersecurity breach caused by a global zero-day vulnerability (the "vulnerability") in the Progress Software MOVEit file transfer program used by the prescribed person at the time of the breach to perform secure file transfers.[3] The MOVEit software was hosted by the prescribed person on its internal secure file transfer server and was used by the prescribed person to encrypt files transferred between the prescribed person and designated partners.

The vulnerability allowed the threat actors to use the web-enabled portal in the software to bypass administrative user multi-factor authentication, decrypt, access, and copy files. Due to the vulnerability, the server hosting the MOVEit software (the "affected server") was accessed and data that was in the process of being transferred for analysis, quality assurance, and/or allocation to designated partners was exfiltrated.

The prescribed person advised that upon becoming aware of the vulnerability, it immediately deployed the recommended remediation measures. However, due to the nature of the vulnerability, the prescribed person reported that it was not able to prevent the attack.

An in-depth analysis revealed that the files copied during the breach contained the personal health information of approximately 3.4 million people, including approximately 1.4 million pregnant individuals and 1.94 million fetuses/children, from a large network of mostly Ontario healthcare facilities and providers regarding fertility, pregnancy, newborn, and child health care offered between January 2010 and May 2023.

The prescribed person reported that there continues to be no evidence that any of the copied data has been misused for any fraudulent purposes. The prescribed person monitored the internet, including the dark web, for any activity related to this incident and found no sign of the impacted data being posted or offered for sale.

---

[2] Health information custodians can disclose personal health information without individuals' consent to prescribed persons for the purpose of compiling or maintaining their registries. Prescribed persons can use personal health information to compile or maintain their registries and for research. See FAQs - IPC for additional information on prescribed persons.

[3] The prescribed person purchased a license to use the MOVEit file transfer software. As such, at the time of the breach, the prescribed person had a software license agreement with Progress Software in the form of End User Terms and Conditions. The affected data was housed on a server hosted by the prescribed person. No personal and/or personal health information was provided by the prescribed person to Progress Software, nor did Progress Software have access to the prescribed person's secure file transfer server where the affected data was housed.

The prescribed person reported that the vulnerability was not unique to it, nor is there information to suggest the threat actors specifically targeted it. The prescribed person advised that the vulnerability resulted in a global cybersecurity incident that affected thousands of organizations from around the world.

## II. Issues:

As a preliminary matter, it is agreed that the impacted organization is a prescribed person under *PHIPA*, that the data impacted by the breach included records containing personal health information, and that the breach resulted in unauthorized access to personal health information that was in the custody or control of the prescribed person at the time of the attack.

As such, the sole issue in this report is whether the prescribed person responded adequately to the breach.

**Issue 1 - Did the prescribed person respond adequately to the breach?**

Prescribed persons, when confronted with a breach of personal health information, must take appropriate steps in response. These steps include identification of the scope of the breach, containment of the personal health information involved, notification of those affected, and investigation and remediation of the breach. These requirements are set out in the *IPC's Manual for the Review and Approval of Prescribed Persons and Entities* (the *Manual*).[4]

These requirements are substantially similar to those applicable to health information custodians (HICs) when responding to a privacy breach. The IPC guidance to health information custodians on these steps is set out in *Responding to a Health Privacy Breach: Guidelines for the Health Sector* (the *PHIPA Breach Guidelines*).[5] As the same general breach response expectations apply, with some modifications, to prescribed persons responding to a breach of personal health information, I will refer to these guidelines, as well as to the *Manual*, in my assessment of the prescribed person's response to this breach.

As part of my review of this matter at Early Resolutions, I sought information from the prescribed person about its response to the breach with respect to scope, containment, notification, investigation, and remediation. Based on the information provided by the prescribed person, for the reasons that follow, I find that the prescribed person responded adequately to the breach.

***Scope of Impacted Data:***

The prescribed person's analysis of the impacted data determined that the files copied during the breach contained the personal health information of approximately 3.4 million people, including approximately 1.4 million pregnant individuals and approximately 1.94 million fetuses/children.

The personal health information that was copied from the affected server was collected from 242 health care facilities and providers across (primarily) Ontario regarding fertility, pregnancy,

[4] Manual for the Review and Approval of Prescribed Persons and Prescribed Entities - IPC.
[5] Responding to a Health Privacy Breach: Guidelines for the Health Sector - IPC.

newborn, and child health care offered between January 2010 and May 2023. The data exfiltrated included files that were in the process of being transferred for several purposes, including analysis, quality assurance, and/or allocation to authorized partners.

The data exfiltrated included personal information (PI) and personal health information (PHI) such as: name, address, postal code, date of birth, health card number (no version code), lab test results, type of birth and interventions/procedures, pregnancy risk factors, pregnancy and birth outcomes, and other attributes of the person and/or course of care, for example height and body mass index. Some of the exfiltrated data was codified with arbitrary codes, for example mental health diagnosis and other data elements collected for which submissions must conform to a predetermined list of options. The data types impacted varied for each affected individual.

The exfiltrated data did not include health card version codes, expiry dates, the 9-digit security numbers on the back, or scans of the cards, credit card, banking, or financial information, social insurance numbers, or patient email addresses or passwords.

Based on the information provided, I am satisfied that the prescribed person took reasonable steps to ascertain the scope of the breach and has provided adequate information about the number of individuals affected by the incident and types of personal health information impacted.

***Discovery and Containment of the Breach:***

On May 31, 2023, Progress Software (the "Vendor") sent a security advisory to the prescribed person regarding the vulnerability. Following receipt of the security advisory, the prescribed person confirmed the exploitation and data extraction through an analysis of the MOVEit file transfer logs, the secure file transfer server, and the end-point detection system. The prescribed person immediately employed the remediation measures provided in the security advisory to neutralize the vulnerability.

To contain the breach, the prescribed person disabled access to the affected server and took it offline. Out of an abundance of caution, the prescribed person's information system, housed in a separate data centre on different servers, was also taken offline and shut down to mitigate the risk of lateral movements and additional attacks by the threat actors.

On the same date, members of the prescribed person's executive leadership team were notified of the exploitation of the vulnerability. The prescribed person also notified its insurer and retained outside counsel who specialize in breach management ("breach counsel"). The prescribed person also engaged third-party cybersecurity experts to assist in its investigation efforts.

On June 1, 2023, the prescribed person's third-party cybersecurity experts were able to extract evidence confirming exploitation of the affected server. Additional analysis verified the exploitation of the MOVEit software web portal and presence of a persistent web shell, sensitive data access, and exfiltration of data two days after the initial exploit, but before the prescribed person was alerted to the vulnerability by the Vendor.

The prescribed person then audited all users who had access to both the affected server and its information system. The passwords of those individuals were reset as a precautionary measure to mitigate the risk of additional exploits.

The prescribed person's third-party cybersecurity experts found no evidence of any lateral movement by the threat actors outside of the affected server. As a result, they issued an attestation letter confirming the safety of the prescribed person's information system on June 5, 2023. On the same date, following a review of the attestation letter by the prescribed person and its breach counsel, the prescribed person's information system was determined to be safe and brought back online.

Although the prescribed person applied all recommended remediation measures, access to the web-accessible portal functionality of the MOVEit software, which was the source of the vulnerability, was disabled and the affected server was decommissioned.

The prescribed person advised that it did not make contact with the threat actors at any time. Additionally, the impacted data files remained fully accessible to the prescribed person at all times.

Based on the information provided, I am satisfied that the prescribed person took reasonable steps to contain the breach following its discovery.

***Notification Efforts:***

As a preliminary matter, prescribed persons generally do not directly notify individuals whose personal health information has been breached while in its custody or control. Instead, the prescribed person is expected to notify the health information custodians or organization who provided the personal health information to it so that the custodian can notify the affected individual in accordance with section 12(2) of *PHIPA*. This is set out in the *Manual*, which provides as follows:

> …as a secondary collector of PHI, a PP or PE should not directly notify the individual to whom the PHI relates of a privacy breach. Where applicable, the required notification to individuals must be provided by the relevant custodian(s), unless an alternative decision regarding breach notification to affected individuals is approved by the IPC.

However, in this case, the scope and unique circumstances of the breach called for an alternative approach to notification, namely one led directly by the prescribed person, which was approved by the IPC in advance of notification in accordance with the *Manual*.

After consultation with the IPC, the prescribed person engaged in the following efforts to notify public bodies, affected health information custodians, and affected individuals about the breach.

Initial Notifications:

Following the incident, the prescribed person notified:

- The Ontario Provincial Police on June 1, 2023;
- The Ministry of Health and Ontario Health on June 1, 2023;
- The IPC on June 5, 2023; and
- Affected Heath Information Custodians on June 6, 2023.

Additionally, the prescribed person posted a public facing statement on its website beginning on June 7, 2023. On the same date, the prescribed person implemented a dedicated call centre to provide basic information to the public.

Notice to Affected Health Information Custodians:

In the event that personal health information provided to prescribed person is stolen, lost, or collected, used, or disclosed without authority, the *Manual* requires the prescribed person to notify the health information custodian that provided the data of the incident at the first reasonable opportunity.

The prescribed person notified impacted health information custodians of the incident on June 6, 2023. Additionally, starting on June 28, 2023, the prescribed person sent affected health information custodians and other partners an update on its investigation along with site specific information about the volume and scope of exfiltrated data. Health information custodians were also invited to information Townhalls (webinars) hosted by the prescribed person in conjunction with external breach counsel and the prescribed person's insurer. Townhalls were conducted on July 5, 7, 10, 17, and 19, 2023.

Notice to Affected Individuals:

After careful consideration, the prescribed person opted to pursue a centralized and coordinated *indirect* notification process, in conjunction with impacted health care providers, to ensure affected individuals received clear, consistent, and safe messaging about the breach, and were provided multiple, equitable avenues for additional information.

In coming to the decision to indirectly notify impacted individuals of the breach, the prescribed person considered the sensitivity of the data that was breached, the fact that a link to the prescribed person via a direct notice would infer past-pregnancy, and the possibility of re-traumatizing those who had an undisclosed or unfavourable history of pregnancy or birth via a direct notice.

The prescribed person also considered the unique structure of the impacted data. For example, in many cases, 3-6 health information custodians contributed the same information to the same individual's record, per birth or pregnancy, meaning that a decentralized direct notification process led by individual health information custodians would have resulted in affected individuals receiving multiple notices from different organizations pertaining to the same compromised records.

Other relevant factors considered included the significant number of affected parties (approximately 3.4 million) and the likelihood of outdated contact information for a percentage of affected parties given that the affected data went back to 2010.

After considering the above variables, the prescribed person determined that a centralized indirect notice process, led by the prescribed person working in conjunction with health information custodians, that allowed for self-identification by affected parties, would be the safest and most effective means of providing notification to the affected class.

*Indirect Notice Process:*

The prescribed person notified affected individuals about the breach on September 25, 2023, after consulting with and obtaining approval from the IPC.

The prescribed person's indirect notice process included the following elements:

1. Public notification using media and health information custodian websites indicating the nature of the incident and direction to visit the prescribed person's incident website.
2. Multi-lingual translated incident website for more information, with self-identification questions to allow individuals to determine if they were impacted by the incident.
3. Hotline for questions (English and French) Monday to Friday 8am-4pm ET.
4. Escalation to the prescribed person's agents for more detailed questions, as required.

The prescribed person's indirect notice process rollout included the following stages and steps:

Pre-notification:

- Notice content was prepared for the prescribed person and health information custodians, including microsite content, FAQs, news release, statements for websites, and on-site postings;
- Microsite development, including content in 5 languages;
- Phone hotline script development;
- Key message development; and
- Stakeholder briefing.

Notification:

- News release distribution on Newswire services on September 25, 2023;
- Microsite incident website launch on September 25, 2023 (end date: February 12, 2024);
- Health information custodian statements went live on their websites and at physical premises on September 25, 2023 (end date: December 31, 2023);
- Phone hotline activation on September 25, 2023 (end date: January 31, 2024);
- Daily media, social, hotline and web traffic monitoring reports; and
- Media interview coordination.

Post-notification

- Continued daily monitoring of traditional and social media;
- Daily web analytics from third-party vendor; and
- Daily/weekly reporting and escalations from hotline providers.

*Indirect Notice Content:*

The prescribed person's incident website contained an incident summary, a detailed self-identification questionnaire, a list of FAQs, a list of affected data providers, a link to the prescribed person's press release about the incident, and contact information for the prescribed person's dedicated incident call centre, which was available from Monday to Friday, 9am to 5pm, from June 2023 to January 31, 2024.

Based on my review, the prescribed person's incident website contained all elements of patient notification recommended by the IPC in the *PHIPA Breach Guidelines*, including information about the details and extent of the breach, the specifics of the types of personal health information at issue, the steps that had been taken by the prescribed person to address the breach, that the IPC had been notified of the breach, that affected parties have a right to make a complaint to the IPC, and the contact information for the prescribed person's dedicated incident call centre if individuals had any questions.

Analysis of the Prescribed Person's Notice Efforts:

Based on the information before me, I am satisfied that the prescribed person took reasonable steps to notify the affected individuals about the breach.

In coming to this conclusion, I am mindful that it is generally better for health information custodians, or prescribed persons acting in place of health information custodians for notification purposes, to provide direct notification to individuals who may have been affected by a privacy breach. Direct correspondence is more likely to draw the individual's attention to their potential involvement in a breach than a posted notice. However, in this case, given the very large number of individuals impacted by this incident and the unique circumstances of the breach, it was reasonable for the prescribed person to determine that direct notice was not feasible in the circumstances.

A health information custodian that is considering indirect notification should consult with the IPC about its notice plans in advance and be prepared to explain why they believe indirect notice is reasonable in the circumstances, as well as what their plans for indirect notification are. Factors that may weigh in favour of indirect notice may include a significant number of affected parties, likelihood of outdated contact information, and if direct notice is reasonably likely to pose a risk of harm to individuals.

When engaging in indirect notification, health information custodians should ensure they take reasonable steps to bring the indirect notice to the attention of the affected parties. It will rarely, if ever, be sufficient to satisfy the notice obligations of the *Act* for a health information custodian to post an indirect notice to their website, without taking further steps to bring the notice to the

attention of the affected class. This is because the affected parties may not routinely access the custodian's website, and therefore would be unlikely to encounter the website notice unless prompted to go there.

Health information custodians undertaking an indirect notice process should carefully consider what forms of public communications are most likely to reach the affected individuals. Thought and care should be put into deciding what strategy will be most effective at reaching the target audience. Multiple methods of public notification will likely be the most effective way to reach affected individuals. A multi-media strategy comprised of media releases, prominent notices on the landing page of the custodian's website, posts on the custodian's social media accounts about the breach, physical on-site postings of the notice in high-traffic areas of the custodian's facility, advertisements in newspapers about the breach, and other case-specific strategies to direct affected parties to the notice should be considered a best practice in these cases.

With respect to the content of an indirect notice, health information custodians should ensure the notice contains fulsome information about the breach and sufficient details to enable someone reading it to easily determine if they were affected by the incident and how. To facilitate this, an indirect notice should clearly identify the categories of patients that were impacted by the breach, over what time period, what information was impacted, and how specifically the information was impacted by the breach. The indirect notice should also contain all elements of patient notification set out in the *PHIPA Breach Guidelines*.

In the case at hand, I am satisfied that the prescribed person took reasonable steps to bring the indirect notice to the attention of affected parties. The prescribed person's efforts in this regard include issuing a news wire release about the incident that resulted in widespread coverage of the incident, requiring the 242 affected health care providers to post and maintain a notice about the incident on their websites and in their physical facilities for a minimum period of 90 days, and establishing a dedicated incident website that remained live for four and a half months following notice to affected parties of the breach.

I am further satisfied that the prescribed person took reasonable steps to ensure the indirect notice contained fulsome information about the incident and provided sufficient details to enable an individual reading it to determine if and how were they affected. In coming to this conclusion, I reviewed the information available on the prescribed person's incident website, which amongst other things, contained a detailed self-identification questionnaire that allowed individuals to determine personal impact. For those who wanted additional information or clarification about the breach, a dedicated incident hotline was available Monday to Friday for four months following breach notification.

***Investigation and Remediation of the Breach:***

The IPC's *PHIPA Breach Guidelines* state that the investigation and remediation of a breach should include both a review of the circumstances surrounding the breach and a review of the adequacy of existing policies and procedures in protecting personal health information. This is consistent with the requirements imposed on prescribed persons following a breach as set out in the *Manual*.

Investigation of the Attack:

The prescribed person engaged third-party cybersecurity experts to assist in its investigation efforts. Based on its investigation, the prescribed person determined the threat actors began their initial attack on the affected server on May 28, 2023. On that date, they exploited a SQL injection vulnerability (CVE-2023-34362) to gain unauthorized access to the affected server via escalated privileges. Specifically, the threat actors created a backdoor by deploying a newly discovered web shell human2.aspx that masqueraded as human.aspx, a legitimate component of the MOVEit file transfer software application. No data was exfiltrated during this initial attack.

On May 31, 2023, the threat actors exfiltrated roughly six gigabytes of data across 120 files. This occurred approximately two hours before the Vendor sent the security advisory to customers, including the prescribed person, warning them of the vulnerability.

The prescribed person's investigation suggested the threat actors copied the data at approximately 12:30 p.m. EST on May 31, 2023. The Vendor sent the initial security advisory at approximately 2:00 p.m. EST on May 31, 2023. This notification was quarantined due to the prescribed person's email security mechanisms.

The prescribed person reported that the breach was contained on or about 6:00 p.m. on May 31, 2023. The prescribed person advised that there is no evidence to suggest the threat actors successfully accessed the affecter server after 12:30 p.m. on May 31, 2023.

Based on the information provided, I am satisfied that the prescribed person took reasonable steps to investigate the circumstances surrounding the breach and has adequately determined its root cause and the series of actions taken by the threat actor during the attack.

Remediation Efforts:

This breach was caused by a zero-day vulnerability in the MOVEit software web portal, which was exploited by the threat actors to gain access to the personal health information stored on the prescribed person's secure file transfer server.

Following the breach, the prescribed person disabled the web-portal, decommissioned the affected server, and discontinued its use of the MOVEit file transfer software.

Subsequently, the prescribed person selected a new secure file transfer software provider.[6] In selecting its new secure file transfer provider, the prescribed person reviewed industry standards and consulted with other prescribed persons and prescribed entities about their secure file transfer services. Following this initial due diligence, the prescribed person consulted with external security experts who confirmed that the selected provider was an appropriate choice for the

[6] Similar to MOVEit, the prescribed person purchased a license to use the new secure file transfer provider's software only. The new vendor does not have any access to the prescribed person's data as the file transfer solution is hosted in the prescribed person's own environment.

prescribed person based on industry standards and the prescribed person's needs. The prescribed person advised that web portal access was not required for this implementation.

Penetration testing was performed, and the recommendations stemming from that exercise aided in the configuration of the new system. For example, the prescribed person is implementing a multi-layer security architecture deployment for the secure file transport solution, the details of which were provided to the IPC but will not be shared publicly for security reasons.

Additionally, the prescribed person reported that going forward, all analytical services will be contained within the prescribed person's environment. Further, all software and data will only be available via VPN connection.

Based on the information provided, I am satisfied that, following the breach, the prescribed person took reasonable steps to remediate this incident and to enhance its security posture against further attacks of this kind.

Review of Existing Privacy Practices and Procedures:

Pursuant to subsection 13(2) of Regulation 329/04 under the *Act*, the IPC is responsible for reviewing and approving, every three years, the practices and procedures implemented by an organization designated as a prescribed person under clause 39(1)(c) of the *Act*. Such practices and procedures are required for the purposes of protecting the privacy of individuals whose personal health information such organizations receive and maintaining the confidentiality of that information.

This office's expectations of prescribed persons under section 39(1)(c) of *PHIPA* are set out in the *Manual*. The *Manual* is the core document that describes the practices and procedures that this office expects prescribed persons and prescribed entities to have in place.

Among other things, the *Manual* requires that, at a minimum, prescribed persons and prescribed entities develop and implement an overarching information security policy and that this policy "must require that steps be taken that are reasonable in the circumstances to ensure that the personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal." This mirrors the obligation imposed by section 12(1) of *PHIPA* on health information custodians.

At the time of the breach, the prescribed person's privacy and security practices were detailed in Version 3.1.1 of its Privacy and Security Management Plan (PSMP). These practices were approved by the IPC as part of its triennial review process[7] on October 31, 2020, for a three-year period ending on October 31, 2023. The prescribed person's privacy and security practices were most recently reviewed and re-approved by the IPC on October 31, 2023, for a three-year period

[7] Information and documentation pertaining to the IPC's review and approval process for prescribed entities and persons under *PHIPA* can be found at Reviews and Approvals: Documentation | Information and Privacy Commissioner of Ontario (ipc.on.ca).

ending on October 31, 2026. These are set out in version 3.2.2 of the prescribed person's PSMP and include the recommendations from the IPC stemming from its more recent triennial review.

The privacy and security policies within the prescribed person's PSMP that are most relevant to this incident include the following:

- P-29, P-29A, and P-29B (Privacy Breach Management, Breach Management Protocol, and Breach Reporting Form);
- P-30 (Log of Privacy Breaches);
- S-05 (Secure Retention of Records of Personal Health Information);
- S-07 (Secure Transfer of Records of Personal Health Information);
- S-10 (Logging, Auditing, and Monitoring Privacy and Information Security Events);
- S-11 (Vulnerability and Patch Management);
- S-17 (Information Security Breach Management); and
- S-18 (Log of Information Security Breaches).

Following the breach, in direct response to the incident, the prescribed person made updates to the following policies:

- S-05: This policy was updated to include a requirement that files housed on the secure file transfer server must be removed within a prescribed time period.
- S-07: This policy was updated to reflect the prescribed person's new secure file transfer provisioning process, which involves a variety of additional security controls.

Based on the information before me, I am satisfied that following the breach, the prescribed person reviewed the adequacy of its existing privacy and security practices and updated relevant practices and related policies in order to enhance its ability to protect personal health information from breaches of this nature.

I am further satisfied that the prescribed person's privacy practices are consistent with the expectations of our office when reviewing cybersecurity breaches of this kind. Specifically, upon review of the prescribed person's privacy and security policies and the information provided by the prescribed person during the processing of this file, I am satisfied that the prescribed person has adequate measures in place with respect to incident prevention, incident management, and detecting and deterring remote exploit attacks.

The prescribed person's incident prevention practices including annual mandatory cybersecurity training, identity and access management policies and procedures (S-01, S-03, S-05), practices and procedures for logging, monitoring, and auditing of system events in order to proactively detect and respond to potential security concerns (S-10), and practices for protecting data at rest and in transit, including 256-bit AES encryption of all data on the secure file transfer server.

The prescribed person's incident management practices include policies and procedures for responding to privacy and security breaches (P-29, P-29A, P-29B, P-30, S-17, S-18), which detail the steps to take in response to a breach and the staff responsible for executing each step, as well

as measures to test its incident response and security posture and keep them up to date, including annual tabletop exercises, privacy impact assessments, and threat risk assessments.

The prescribed person's practices for detecting and deterring remote exploit attacks include end point detection and response tools across all endpoints on the network, CIS benchmark security hardening measures for virtual systems, and continuous vulnerability scanning of all systems. Further measures include a vulnerability and patch management policy (S-11) and threat intelligence measures, including proactively obtaining and monitoring intelligence related to current and new cyberthreats, tactics, and targets.

## III. Conclusion and Recommendations

After considering the circumstances of this reported breach and the actions taken by the prescribed person, I am satisfied that the prescribed person responded adequately to the breach and that no further review of this matter is required.

Specifically, I am satisfied that the prescribed person has taken appropriate steps to contain and investigate the breach, as well as to notify the affected individuals. I am further satisfied that the prescribed person has adequately remediated the breach and has demonstrated that it has sufficient privacy and cybersecurity practices in place to prevent further incidents of this kind. However, the IPC may re-open this matter if additional information comes to our attention suggesting a need for further inquiry.

The IPC urges the prescribed person to review and follow the guidance set out in the IPC's guidance documents *Technology Fact Sheet: Protecting Against Ransomware*, *Technology Fact Sheet: Protect Against Phishing*, *Responding to a Health Privacy Breach: Guidelines for the Health Sector*, *and* *Detecting and Deterring Unauthorized Access to Personal Health Information* to ensure that its practices, policies, and procedures are sufficient to minimize the risk of a similar breach in the future.

The IPC thanks you for your cooperation in this matter and ongoing commitment to ensure compliance with the *Act*. This letter will serve as confirmation that this file is now closed by the IPC.

Yours truly,

Denise Eades
Analyst