OFFICE OF THE
INFORMATION and PRIVACY COMMISSIONER
for Prince Edward Island

Investigation Report No.	IR-26-001
OIPC File No.	C/25/00011
Custodian	FYi Care Services and Products Inc.
Statute	*Health Information Act*
Report Writer	Tyler Symonds Investigator
Date of Report	June 15, 2026

BACKGROUND

[1] On November 10, 2023, FYi Eye Care Services and Products Inc. ("the Custodian") discovered an unauthorized third-party gained access to a portion of its IT infrastructure. The incident was discovered when IT personnel found encryption within the IT infrastructure. The Custodian hired third parties to investigate, contain, and provide support with regards to the incident response and forensic investigation. The root cause of the privacy breach originated when an IT employee downloaded a trojanized application called Advanced IP Scanner. This application was downloaded to provide remote IT support. At the time of the incident, the Custodian had technical safeguards in place; such as firewalls, password policies, antivirus on all endpoints, regular endpoint and server updates. The breach affected individuals in several other jurisdictions.

INFORMATION

[2] I accept the Custodian's assessment that the personal health information of the affected individuals was stolen in a cybersecurity breach by an unidentified and unauthorized third party.

ISSUE FOR INVESTIGATION

[3] The issue in this review is whether the Custodian took appropriate steps to respond to the privacy breach and safeguard the security and integrity of the personal health information in their custody or control. The Custodian acknowledged that a privacy breach occurred, and the personal health information of the affected individuals was stolen in a cybersecurity breach.

DISCUSSION

[4] When there is a privacy breach, there are several steps a custodian is expected to take in response:

(a) Containment of the breach;
(b) Notifications to affected individual(s) and to the Commissioner;
(c) Investigation of the circumstances of the breach; and
(d) Remediation.

[5] Some of these steps can be, and should be, followed concurrently. For instance, in this matter, the Custodian engaged third parties to investigate, contain, and provide support regarding the incident response and forensic investigation immediately. This continued throughout the process, while other steps were also being undertaken. I will address each step separately below.

Containment

[6] Containment of the breach involves ensuring, if possible, that the personal health information at issue is not subject to further unauthorized disclosure. The forensic investigation determined the incident was caused by downloading a trojanized version of a software application. The date of initial compromise was October 18, 2023, three weeks prior to detection. Prior to deployment of encryption malware, the investigation found evidence of unauthorized access throughout the software, data staging (process of loading data into a temporary storage area) and exfiltration (theft). The Custodian deployed countermeasures to secure the network, such as taking certain systems offline

from the internet. The Custodian also deployed an endpoint detection and response tool to monitor its environment 24/7 and to restrict any further malicious executions.

[7] I find that the Custodian took reasonable steps to prevent further unauthorized access, use or disclosure of personal health information.

Notification

[8] Section 36 of the *HIA* requires that a custodian notify an affected individual and the Commissioner if personal health information is lost or stolen, unless the custodian reasonably believes that the theft or loss will not have an adverse impact on the provision of health care or other benefits to the affected individual, or on the mental, physical, economic, or social well-being of the individual.

[9] In this instance, the review of the data set was completed in June 2024. The Custodian notified affected individuals on January 6, 2025. On January 7, 2025, the Custodian provided notices to applicable privacy regulators. The Custodian offered credit monitoring to the affected individuals.

Custodian Investigation

[10] The forensic investigation determined the incident was caused by an employee downloading a trojanized version of a software application.

[11] The employee of the Custodian was an IT employee that had attempted to download a legitimate application for use in their role to provide remote IT support to other employees. Notifications were made to 14 affected individuals in Prince Edward Island on January 6, 2025.

[12] The Custodian's investigation did not identify any evidence or indication of lateral movement to, or compromise of, the Custodian's patient management system. However, there was evidence of the impact (i.e., theft) of personal health information.

[13] The Custodian conducted a review with third parties to ascertain the scope of impacted individuals and types of impacted personal and personal health information. The review was from March 2024 to June 2024.

[14] The Custodian took various steps to address the factors they determined had led to the privacy breach, and to mitigate against a similar breach happening again. These steps included:

a. Onboarding a comprehensive managed security operations center.

b. Developing a privacy training module that is mandatory for all staff, with regular testing on security awareness to counter potential phishing attempts.

c. Encrypting all laptops and monitoring endpoints using endpoint detection and response (EDR) software (completed) and upgrading firewalls and network segmentation for older endpoints which cannot support EDR.

d. Setting up an internal incident response and phishing control team to investigate potential indicators of cyber incidents.

e. Running a vulnerability monitoring program in cloud, applications and infrastructure, with reviews completed on a weekly basis and remediation items prioritized as applicable.

f. Upgrading server software as applicable.

OIPC Response

[15] I am satisfied that the Custodian responded appropriately to this breach and the steps taken to remediate the situation and protect against a similar occurrence in future were adequate.

[16] The OIPC reviewed Custodian's privacy breach investigation report and followed up with Custodian's legal counsel that conducted the investigation.

CONCLUSION

[17] I find that the Custodian met its obligations under section 39 of the *HIA* to ensure adequate protection and security of personal health information in its custody and control. The Custodian had policies and procedures in place to protect the personal health information in their custody and control and to guard against unauthorized access to, use or disclosure of PHI. The root cause of the unauthorized access was from an IT employee attempting to download a legitimate application for remote work access.

[18] I am satisfied that the Custodian acted appropriately in responding to this serious breach incident, took reasonable steps to contain the breach, and has taken reasonable steps to mitigate against future breaches of a similar nature.

RECOMMENDATIONS

[19] As I am satisfied that the Custodian responded to the breach appropriately, I will make no order in this matter.

Tyler Symonds
Investigator
Office of the Information and Privacy Commissioner for PEI