



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

April 18, 2024

John Babos
Manager, Access and Privacy
Ministry of Health
99 Adesso Drive
1st Floor
Concord, ON L4K 3C7
Email: GeneralAPO@ontario.ca

Dear John Babos:

RE: PR21-00041

The Ministry of Health (MOH) reported a breach of the *Personal Health Information Protection Act* (the *Act* or PHIPA) to the Office of the Information and Privacy Commissioner of Ontario (IPC) in November 2021, and the above-noted file was opened.

The circumstances of the breach involved the theft of 359,663 individuals' personal health information (PHI) from the COVaxON application (online COVID-19 immunization system) by an employee of a vendor contracted by the Provincial Vaccine Contact Centre (PVCC).

Background

The PVCC is responsible for, amongst other duties, booking vaccination appointments, providing proof of vaccination, and tracking vaccine inventory and vaccine dose administration using the COVaxON application. The PVCC contracts vendors to provide a workforce to perform these duties and provide information related to COVID-19 vaccination appointments.

The MOH clarified that it is a health information custodian responsible for the information collected and housed in the COVaxON application by the PVCC, and the Ministry of Public and Business Service Delivery (the MPBSD) is the MOH's agent, as defined by section 17 of the *Act*, that oversees the PVCC.

On November 15, 2021, individuals who had scheduled vaccine appointments or downloaded vaccine certificates through COVaxON received text messages asking for their financial information. A municipal police service notified the Cyber Security Operations Centre (CSOC) of the MPBSD that one of their officers and their spouse received spam text messages related to the PVCC. The CSOC informed the MOH of possible unauthorized access to the COVaxON application, and on November 17, 2021, the MPBSD alerted the Ontario Provincial Police (OPP).



Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel/Tél : (416) 326-3333
1 (800) 387-0073
TTY/ATS : (416) 325-7539
Web : www.ipc.on.ca

Other members of the public also began notifying the MOH and the MPBSD that they received financial spam text messages (SMS¹) asking them to respond and provide personal financial information after scheduling vaccination appointments or downloading receipts through the COVID-19 Patient Portal.

On November 22, 2021, the OPP laid charges against two individuals, one of whom was an employee of a third-party vendor contracted to provide a workforce to the PVCC. The second individual was arrested in Quebec. The OPP estimates that the two individuals sent thousands of spam texts to individuals who interacted with COVaxON.

The OPP investigation found that the names and phone numbers used in the text messages were stolen from COVaxON by the employee of the PVCC's third-party vendor who, as part of his job, was authorized to access and use COVaxON.

The MPBSD and CSOC conducted a security investigation of COVaxON to review internal system activity and use. Analysis of user logs identified suspicious activity in COVaxON search logs and determined that a single authorized user had accessed an unusually large number of records through various searches between November 4 and 20, 2021. The MOH determined that the individual harvested the data by copying and pasting the search results from the search screen in his browser into a spreadsheet on his laptop. The Ministry concluded that the following personal health information (PHI) was breached, combinations of which varied by individual:

- Name
- Phone Number
- Health Card Number (HCN)
- Date of Birth (DOB)
- Email Address
- Clinic where COVID-19 vaccine was received or planned to be received

In over 95% of the cases, a person's name on its own or with their phone number was stolen. Beyond that, the following information made up approximately 5% of the remaining seized information:

- Email Address
- Health Card Number (HCN)
- Date of Birth (DOB)
- Clinic where COVID-19 vaccine was received or planned to be received.

Issues and Discussion:

It is the position of the MOH that, under the *Act*, it is a "health information custodian" in relation to the records of PHI collected and maintained by the PVCC and that the individual who stole PHI from the PVCC and his employer (the third-party vendor) were "agents" of the MOH, as defined by section 17 of the *Act*.

¹ SMS or Short Message Service, commonly known as texting, is a way to send text-only messages to phones.

Based on the information before me, I agree that the MOH is a “health information custodian” under section 3(1) of the *Act*; the records that were inappropriately accessed and in the custody or control of the Ministry contained “personal health information” within the meaning of section 4(1) of the *Act*; the individual who stole PHI from the PVCC and his employer (the third-party vendor) were “agents” of the MOH as defined in section 2 of the *Act*; and, as a result of the unauthorized accesses by its agents, PHI was used and disclosed contrary to Part IV of the *Act*.

The following issues were identified during the review of this breach file at the early resolution stage:

- 1) Did the MOH take adequate steps to contain the breach?
- 2) Did the MOH take adequate steps to notify individuals who were affected by the breach?
- 3) Did the MOH take reasonable steps to protect the personal health information (PHI) collected through the PVCC?
- 4) Did the MOH take reasonable steps to ensure that the conditions or restrictions imposed on the collection, use and/or disclosure of PHI by its agents were in accordance with section 17 of the *Act*?
- 5) Did the MOH take reasonable remedial measures that will likely prevent similar breaches in the future?

Issue 1 - Containment

The MOH submits that it is confident that this privacy breach was quickly contained given the OPP’s seizure of the accused’s laptops within days of the first spam text message being sent out.

Because the alleged perpetrators were arrested and their laptops seized within a week of the breach being identified, and as no more financial spam messages were sent out from them afterwards, the OPP and the ministries (the MOH and the MPBSD) reasonably believe that the breach was quickly contained.

The MOH submits that the purpose of the PVCC data theft was to steal the names and phone numbers of Ontarians (representing over 95% of impacted people). This personal information was then used to send the SMS spam text messages to the affected individuals to prompt them to send the alleged perpetrators money. Considering the OPP noted that no one had contacted them about the sharing of their financial information in response to the spam texts, the MOH advised that the risk of identity theft/fraud is very low.

In the circumstances, it does not appear that there are any outstanding containment issues to be addressed by the MOH.

Issue 2 - Notification to Affected Parties

Under section 12(2) of the *Act*, a health information custodian must notify individuals affected by a breach at the first reasonable opportunity.

The MOH advised that due to the criminal investigation by the OPP, details of the breach were not known to the MOH during its investigation, which caused a delay in the MOH's breach notification to the affected individuals.

The MOH advised that the OPP investigation was important to quantify the scope of the breach by identifying the names of affected individuals from evidence seized from the accused's computer equipment to enable an informed notification process.

In February 2022, the OPP provided a list of the names of all affected individuals that could be ascertained to the ministries for their notification work. Knowing only the names of individuals and with no other qualifiers, the MOH and the MPBSD were unable to confidently identify those affected by the breach. In the summer of 2022, the OPP advised that they could provide additional data to allow for more targeted notifications of the privacy breach.

The MOH sent notifications to 359,019 affected individuals between December 9 and 14, 2022 using email, mail, and auto-dialer/phone.

There were 644 affected individuals who had no contact information in the system and thus received no breach notification.

Where breach notifications to the affected individuals were unsuccessful (e.g., email rejected as 'undeliverable'), a second notification to 11,512 people via mail or auto-dialer/phone began on May 22, 2023, and was successfully completed on May 25, 2023.

The breach notification contained the following information:

- The details and extent of the breach;
- The specifics of the personal health information at issue;
- The steps that have been taken to address the breach;
- That the IPC was notified of the breach, and referral to the IPC website should the individual want to file a privacy complaint; and
- The contact details of the person within the MOH that the individual should contact if they have questions.

In the circumstances, I am satisfied with the steps taken by the MOH to notify the affected individuals. While it is important for custodians to notify affected individuals "at the first reasonable opportunity," under the *Act*, I acknowledge the extenuating circumstances connected to the OPP investigation that prevented a timelier notice.

Issue 3 - Did the MOH take reasonable steps to protect the personal health information (PHI) collected through the PVCC?

Under section 12(1) of the *Act*, health information custodians must ensure that PHI is reasonably protected against theft, loss, and unauthorized use or disclosure, and to ensure that the records containing the information are protected against unauthorized copying, modification, or disposal.

Prior to the breach, the MOH had the following measures in place to protect the PHI held by the PVCC:

- The PVCC conducted Criminal Records and Judicial Matters checks on its employees and its vendors' employees prior to hire. The PVCC also provided training to its employees and its vendors' employees upon hire regarding their privacy obligations under the *Act*. The PVCC also required employees and agents to sign a confidentiality agreement (CA) to acknowledge their privacy obligations and their agreement to safeguard personal information and personal health information.
- The vendor ensured the above-noted criteria were met for each employee through tracking and recording before the MOH and MPBSD provided Ontario Public Service (OPS) equipment and systems to PVCC employees/agents to perform their job role.
- Each morning prior to their phone lines opening to the public, the PVCC verbally reminded its employees and its vendors' employees to keep individuals' PHI confidential.
- The PVCC randomly audited employees' calls for quality control and privacy compliance.
- In order to sign in to COVaxON, an employee had to complete a multifactor authentication process as well as acknowledge a privacy warning.

These measures are consistent with the privacy best practices noted in IPC guidance document "Detecting and Detering Unauthorized Access to Personal Health Information,"² with the following exceptions:

- Although all PVCC staff and agents are required to complete their privacy training and confidentiality agreements upon hire, they were not required to renew their confidentiality agreements annually.
- Although the PVCC randomly audited employees' calls for quality control and privacy compliance, it did not appear that staff and agents' accesses to the COVaxON database were monitored and audited. Logging, auditing, and monitoring is an effective deterrent to unauthorized access if all agents are made aware that all of their activities in relation to electronic records of PHI will be logged, audited, and monitored on an ongoing, targeted, and random basis.

I will recommend that, going forward, all staff/agents of the PVCC should complete mandatory privacy training and confidentiality agreements both at hire and annually thereafter so that they are reminded of their privacy obligations under the *Act* and the rules and information practices of the MOH.

Issue 4 - Did the MOH take reasonable steps to ensure that conditions or restrictions imposed on the collection, use, and/or disclosure of PHI by its agents were in accordance with section 17 of PHIPA?

It is important to note that the PVCC provides its staff and agents with the equipment it requires to do the job they are required to do. The PVCC also permits its staff and agents to access the COVaxON application and database using the assigned equipment to perform their work

² [Detecting and Detering Unauthorized Access to Personal Health Information - IPC](#)

functions. Contractual agreements with vendors entrusted with access to personal information and personal health information are an important part of ensuring compliance with section 17 of the *Act*. The MOH has a Strategic Sourcing Agreement (contract) with the vendor that provides the PVCC workforce, and includes the following criteria:

- Confidentiality requirements for protecting personal information from unauthorized collection, use, disclosure, or destruction by staff/agents;
- A prohibition on copying confidential information; and
- Use and access restrictions that outline compliance obligations.

PHIPA Decision 110³ outlines the importance of having a contractual agreement that details the privacy obligations and expectations of independent contractors who will be entrusted with access to PHI in the custody and control of health information custodians as set out in the *Act*. Similarly, Privacy Complaint Report PR16-40⁴ discusses the importance of an institution having a detailed contract with any third-party vendor that performs core functions on its behalf to ensure compliance with the institution's rules, information practices, and obligations as set out in the *Freedom of Information and Protection of Privacy Act (FIPPA)*.

Audits are another necessary and important way to ensure adequate oversight and compliance with an institution's rules and obligations. Consequently, implementation of audits should also be expressly stated and made enforceable under the terms of any agreement/contract with a vendor. Had regular audits of staff user activity occurred, the prohibited actions of the employee/perpetrator may have been caught immediately, possibly preventing the theft of PHI from the COVaxON application.

The MOH submits that the COVaxON database uses a certain software as its underlying platform, and that it is not technically possible to prevent users from copying data from the software's user interface screen that enabled this breach to occur. To mitigate this vulnerability, the MOH has implemented other remedial measures to address the platform's vulnerability of data exfiltration.

It is clear that remedial measures should be taken to strengthen the MOH's privacy posture when engaging with third parties to provide services involving the handling of PHI under the *Act*. These remedial measures are discussed in the "Recommendations and Next Steps" section below.

Issue 5 - Did the remedial measures implemented by the Ministry satisfy the IPC that they will likely prevent similar breaches in the future?

After the breach, in early 2022, the PVCC provided its employees and its vendors' employees with refresher privacy training and required all employees to attest to their retraining. The PVCC's privacy training covered employees' responsibility to collect, use, or share personal

³ [PHIPA DECISION 110 - Information and Privacy Commissioner of Ontario \(ipc.on.ca\)](https://www.ipc.on.ca/decisions/110)

⁴ [PR16-40 - Information and Privacy Commissioner of Ontario \(ipc.on.ca\)](https://www.ipc.on.ca/decisions/pr16-40)

health information only as authorized under PHIPA (or FIPPA). Further, PVCC staff and agents were required to redo their privacy training and confidentiality agreement (CA) after this breach.

In order to sign in to COVaxON, an employee must complete a multifactor authentication process as well as acknowledge a privacy warning. Since the breach, the MOH has updated the permission settings on COVaxON, limiting what data and functions an employee can access so that they cannot retrieve and retain as much information as the perpetrator did in this breach.

The COVaxON search functionality was changed as follows:

- Search page changes: The original client search page was disabled in favour of a new client search screen. The original client search page provided a “fuzzy” search algorithm using demographic fields for the client. The new search screen imposed a new user workflow that first presents the user with a field to enter the client health card number (HCN). Only if the HCN search does not yield an exact match is the user presented with the fuzzy logic fields.

The COVaxON system does not support the use of wild cards, but the fuzzy logic will retrieve more than just direct matches. The fuzzy logic algorithm is an important feature that helps avoid creating duplicate client records.

- HCN Masking: The HCN returned in the client search is now masked to show only the last four digits.

Subsequent to the above changes, PVCC user training was enhanced to reinforce the new search workflow.

Other security mechanisms were implemented to prevent employees from exfiltrating data. The MOH requested that the MPBSD’s Cyber Security Operations Centre monitor the COVaxON application through their 24/7 enhanced monitoring program that can identify:

- Suspiciously high counts of records accessed by COVaxON user accounts.
- Multiple IPs accessing a single account. (Internet Protocol is the communication standard used to uniquely identify systems on a computer network or across the internet. Networked systems are each assigned an IP address, which is used to uniquely identify and locate that system for the purpose of data transmission.)
- Suspiciously high counts of login status errors.

Additionally, access to the Application Programming Interface for the COVaxON database is now limited to a specific user profile.

The steps outlined above demonstrate reasonable remediation measures to prevent future breaches, subject to the recommendations made below.

Recommendations and Next Steps

Contractual agreements are key to ensuring that third-party vendors and their employees are aware of their privacy obligations under the applicable legislation when entrusting the personal information and/or personal health information held by a custodian to a third party. Based on the

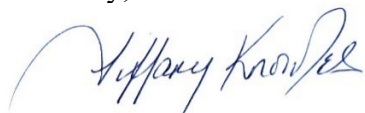
information provided by the MOH, it is not clear how the PVCC confirms that the vendors' data handling capabilities of PI and/or PHI are in compliance with the contract terms referenced above or with the collection, use, and disclosure requirements of the *Act*. I recommend that at the first reasonable opportunity, the MOH ensures that it implements the following with regard to its relationship with third-party vendors for the PVCC:

1. Ensure that the MOH require proof from a vendor that staff who have authorized access to the COVaxON application have completed privacy training and signed confidentiality agreements annually, not just at hire, in order to educate and remind staff of their obligation to comply with the custodian's rules, information practices, and privacy obligations under PHIPA. The completion dates of these mandatory privacy requirements by PVCC staff/agents should also be tracked and recorded to confirm compliance.
2. Ensure that its vendors and their staff understand that exfiltration of data from the COVaxON application is strictly prohibited. This prohibition should be explicitly reviewed with the vendor and form part of its annual privacy training with staff/agents going forward.
3. Ensure that the MOH/MPBSD conduct regular 'user' audits of employees'/agents' access to the COVaxON to confirm that their access and use of the data are in compliance with PHIPA. A formal record of the details/findings of these user audits should also be a requirement.

The MOH has since confirmed its agreement to implement the above-noted remedial actions recommended by the IPC to ensure that a similar incident does not occur in the future. In fact, some of these remedial actions are already in place.

After considering the circumstances of this reported breach, I am satisfied that no further review of this file is required. This report will serve as confirmation that this file is now closed.

Sincerely,



Tiffany Knowles
Analyst