SPECIAL REPORT 23-04

Follow-up report

Left untreated:

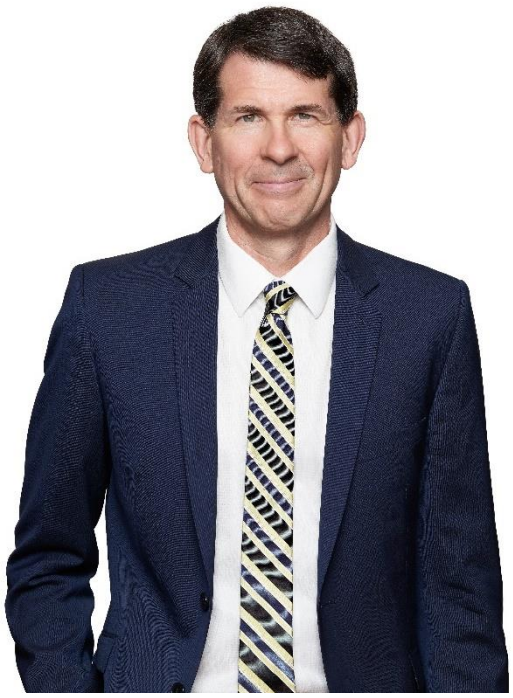
Security gaps in BC's public health database

SEPTEMBER 2023
CANLII CITE: 2022 BCIPC 81
QUICKLAW CITE: [2022] B.C.I.P.C.D. NO. 81

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Table of Contents

Commissioner's Message



As digital innovation continues to transform health care provided in Canada and abroad, British Columbians find increasing amounts of their sensitive personal information being collected and stored within digital systems. From personal health numbers to records relating to individuals' mental health status, British Columbia's Provincial Public Health Information System stores large amounts of sensitive information about those of us accessing healthcare and communicable disease services.

Not only is the information stored within the Provincial Public Health Information System highly personal and sensitive, but the security of the System itself is also critical to British Columbians' ability to access quality care. It was for this reason that in 2022 my office initiated an investigation into the System's privacy and security protections.

In December 2022, my office published the initial investigation report which included seven recommendations to ensure the continued availability of the province's health care system and the protection of individuals' information and privacy rights.

I am pleased to report that the Provincial Health Services Authority (PHSA), the body tasked with operating the Provincial Public Health Information System, has taken meaningful steps to strengthen the privacy and security of the System. While there is more work to be done, I am encouraged by the PHSA's efforts and commitments to addressing the recommendations of my office and ensuring the trust of British Columbians in the health System.

All public bodies and organizations can leverage the findings of the initial report and this follow-up to ensure they are taking reasonable steps to protecting the personal information with which they are entrusted.

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

Executive Summary

Public bodies are required to protect personal information in their custody or under their control by making reasonable security arrangements against risks such as unauthorized collection, use, disclosure, or disposal or personal information.[1] The Provincial Health Services Authority (PHSA) is the body charged with operating the Provincial Public Health Information System (referred to in this report as the System) and ensuring the appropriateness of the System's privacy and security protections.

The System collects large volumes of highly sensitive personal information about all British Columbians relating to the delivery of healthcare and the management of outbreaks of communicable diseases. During the initial investigation, the Office of the Information and Privacy Commissioner for British Columbia (OIPC) found that given the volume and sensitivity of personal information in the System, the PHSA did not have adequate safeguards in place to properly protect the personal information within the System.

The OIPC made seven recommendations to address the identified gaps relating to: privacy-tailored security information and event management, security architecture, application vulnerability management, encryption of personal information, penetration testing, secure desktop environments and Identity Risk assessment and Identity Assurance.

Six months after the release of the report, the OIPC began reviewing the PHSA's implementation of the recommendations. As this report details, the PHSA has taken positive steps to address the recommendations. Two matters have now been fully implemented with the PHSA continuing implementation work to ensure the balance of the recommendations are addressed so that the province's health system is properly secure and protected.

[1] FIPPA, s. 30.

Background

In December 2022, under the authority of s. 42 of the *Freedom of Information and Protection of Privacy Act* (FIPPA), the Office of the Information and Privacy Commissioner (OIPC) conducted an investigation into whether the Provincial Health Services Authority (PHSA) had the necessary security and privacy measures in place to protect personal information stored in the Provincial Public Health Information System (referred to as the System). The System collects significant volumes of sensitive personal information about all British Columbians, to facilitate the delivery of healthcare and to manage outbreaks of communicable diseases.

The investigation focused on the technological controls the PHSA had in place to protect personal information and found that given the sensitivity of personal information in the System, the controls in place fell far short of what was reasonably necessary to protect the privacy of members of the public. The OIPC made seven recommendations to the PHSA, including:

1. Acquire, configure, and deploy privacy-tailored security information and event management technology that is supported by appropriate staffing to maintain the technology and to conduct privacy investigations.
2. Produce and maintain a comprehensive written security architecture document that includes system security requirements, controls design documentation and operations manuals for each component of the system. Ensure the document is signed and approved by senior officials at the PHSA and use it to form the basis for an annual security audit.
3. Implement an ongoing application vulnerability management program to monitor for risk exposures related to unpatched software, and regularly report those to senior management.
4. Evaluate implementing the encryption of personal information within the Database.
5. Conduct penetration testing at least once per year, then report the results and mitigation plans to the Ministry within three months of the completion of the penetration test.
6. Ensure that only secure desktops can access the System or ensure the security of the System cannot be compromised by unsecure desktop environments with access to the System.
7. Conduct an Identity Risk assessment to determine the appropriate level of Identity Assurance required of the System. The PHSA should ensure that all organizations accessing the System use an authentication solution that meets the assurance level required.

Six months later, the OIPC began its follow-up with the PHSA on their implementation of the recommendations. In addition to their written responses, the OIPC requested the PHSA provide supporting documentation to demonstrate the progress reported. This follow-up report highlights the PHSA's progress as of August 1, 2023.

Findings & Recommendations

The PHSA has taken steps toward implementing each of the seven recommendations provided within the initial investigation. Two recommendations have been fully implemented, three recommendations have been substantially implemented, and the remaining two recommendations have been partially implemented. In this context, substantially implemented means that the PHSA has made significant progress to address the recommendation and has committed to fully implementing the recommendation within a defined period. Partially implemented means that the PHSA has made some progress to address the recommendation, but must take additional steps to develop a comprehensive action plan and fully implement the recommendation.

The PHSA's progress with respect to each recommendation is outlined below. As many of the details of the PHSA's progress are technical and sensitive in nature, only a summary of the progress is provided.

Recommendation 1

> ***Recommendation 1**: Acquire, configure, and deploy privacy-tailored security information and event management technology that is supported by appropriate staffing to maintain the technology and to conduct privacy investigations.*

Status: Substantially Implemented

The PHSA procured a contracted vendor in January 2023 to deliver a lifecycle privacy monitoring solution (hereafter referred to as the solution) to enable the PHSA to implement proactive privacy and security auditing of the System.

The PHSA has since initiated the integration of the solution (for example, through completing network connectivity configuration between the vendor and the PHSA, completing web management console connectivity, etc.) and plans to complete the integration by August 31, 2023.

The PHSA has also reported that additional internal resources have been allocated to maintain the technology and to conduct privacy investigations. The resources include, for example, a Privacy Officer, an Information Security Integration Specialist, and a Working Group to support the work of privacy investigations.

The PHSA's contract and associated support agreement with the vendor appear robust and should expedite the ability of the solution to produce proactive intelligence and identify potential privacy breaches.

This is an immense task given the complex, and at times seemingly random, usage patterns within the Database. The OIPC expects it will take the PHSA several months after the integration is finalized to fine-tune the log and alerting rules of the solution to achieve high-quality results. This tuning period will likely generate large volumes of suspicious event alerts that PHSA will need to investigate and will require PHSA to train and supplement their staffing complement to handle the increased workload related to event alerts and follow-up investigations. The OIPC commends the PHSA for taking the necessary steps to ensure appropriate internal resources are available to support this important work.

The PHSA will provide the OIPC with regular updates as they continue to finalize the integration of the solution and work toward achieving high-quality results that will enable the PHSA to fully address this recommendation. The PHSA will also provide a demonstration of the solution once it considers this recommendation to be fully addressed, so that the office can assess the status of the implementation before concluding follow-up.

Recommendation 2

> ***Recommendation 2**: Produce and maintain a comprehensive written security architecture document that includes system security requirements, controls design documentation and operations manuals for each component of the System. Ensure the document is signed and approved by senior officials at the PHSA and use it to form the basis for an annual security audit.*

Status: Substantially Implemented

The PHSA completed a review of all its security architecture, operations manuals and system design documents in existence for the System and developed a single consolidated and standardized document to represent a consolidated security architecture document for the System to be maintained and updated over time.

The consolidated security architecture document was signed and approved by the PHSA's Interim Chief Information Officer, with responsibility for IMIT Information Security and Chief Digital Innovation Officer, Provincial Digital Health and Information Services, with responsibility for the PHSA Enterprise Architecture.

The PHSA's consolidated written security architecture document is comprehensive and includes system security requirements, controls design documentation and operational manuals for each component of the system. However, several security operational documents are in the process of being finalized and are expected to be completed within 2023.

While the architecture document was signed and approved by senior officials at the PHSA, the PHSA has advised that the ultimate responsibility for authorizing future improvements to the System lies with the Ministry of Health. Therefore, the PHSA should ensure that a Ministry of Health Executive responsible for authorizing future improvements also signs the security architecture document.

The importance of executive approval and annual security audits is that without Executive support, future improvements to security and privacy of the System, including those intended to protect the personal information of British Columbians, are at risk. Performing annual audits to confirm that security objectives defined in the architecture document are being met will provide the Executive(s) with the risk assessment necessary to make sound decisions on enhancements. As such, the PHSA should have the security architecture document signed and approved by an Executive responsible for the System.

The PHSA has committed to conducting annual security audits, with the first audit scheduled to be completed March 31, 2024.

The PHSA will provide a copy of the audit report once available. As stated above, the OIPC also recommends the PHSA ensure the architecture document is signed and approved by a Ministry of Health Executive responsible for the System.

Recommendation 3

> ***Recommendation 3**: Implement an ongoing application vulnerability management program to monitor for risk exposures related to unpatched software, and regularly report those to senior management.*

Status: Fully Implemented

The PHSA reported that it has implemented a vulnerability management process by aligning its monitoring with the vulnerability and risk management assessments of the System provided to the PHSA by the Office of the Chief Information Officer for British Columbia. This includes working with multiple service and support providers to identify vulnerable software components and implement a patch management strategy consistent with the BC Government's security standards.

The PHSA has provided documentation demonstrating that initial patching updates to the Operating System and Database Layers were completed between February and May 2023. The PHSA also began reporting on risk management assessments to senior management on December 19, 2022.

The PHSA demonstrated a new commitment to a vulnerability management program to monitor for risk exposures related to unpatched software. While this is an exceptionally difficult task for such an application environment, it is a critical control as outages to the System are not tolerated.

Recommendation 4

> ***Recommendation 4**: Evaluate implementing the encryption of personal information within the Database.*

Status: Fully Implemented

The PHSA's service provider that delivers technical support services for the System completed the encryption of personal information in May 2023. All tables containing personal information within the Database are now encrypted using the internal tools provided by the Database Management System. This is a robust solution that improves the overall privacy and security of the System and the OIPC considers this recommendation to be fully implemented.

Recommendation 5

> ***Recommendation 5**: Conduct penetration testing at least one per year, then report the results and mitigation plans to the Ministry within three months of the completion of the penetration test.*

Status: Substantially Implemented

The PHSA reported that a penetration test was conducted on the System in June 2022 and has committed to performing annual penetration tests by an independent third party. The next penetration test of the system is scheduled to be completed by August 31, 2023.

The PHSA has advised that a report of the results and mitigation plans for the test will be provided to the Ministry of Health within three months of the completion of the test. The PHSA will also provide a copy of the independent penetration test to the OIPC, once complete.

Recommendation 6

> ***Recommendation 6**: Ensure that only secure desktops can access the System, or ensure the security of the System cannot be compromised by unsecure desktop environments with access to the System.*

Status: Partially Implemented

The PHSA presented this recommendation to the System's Data Governance Committee for consideration. The Data Governance Committee is the multi-jurisdictional oversight body accountable for the management of all data held in the System and includes representation from all participating organizations.

The PHSA reported that it is also considering longer-term solutions involving system architecture changes and the implementation of new technology into the System to fully address this recommendation.

In the interim, the PHSA is completing a series of consultations with participating organizations. The PHSA reported that all authorized users are contractually required to comply with security measures and system policies. The consultation process is intended to strengthen privacy and security controls through informing necessary updates to relevant policy language to ensure only secure desktop environments access the System. The PHSA has reported that it expects to complete these updates by January 31, 2024, at the latest.

Given that the participating organizations on the System's Data Governance Committee are extremely diverse and have varying levels of resources available to them, the OIPC supports the approach of addressing this recommendation through Committee. The Data Governance Committee should consider leveraging and sharing existing resources as an effective way to address privacy and security gaps that could impact the System for all users.

The PHSA will provide subsequent progress updates to the OIPC, including when its policy language is updated and when it considers this recommendation to be fully implemented.

Recommendation 7

> ***Recommendation 7**: Conduct an Identity Risk Assessment to determine the appropriate level of Identity Assurance required of the System. The PHSA should ensure that all organizations accessing the System use an authentication solution that meets the assurance level required.*

Status: Partially Implemented

The PHSA has completed a comprehensive risk assessment against the Office of the Chief Information Officer's Identity Assurance Standard and the applicable National Institute of Standards and Technology (NIST) standard.

The PHSA has reported that it, along with the regional health authorities and Providence Health Care Society, has already enabled multi-factor authentication for external remote access. All remaining participating organizations are working to implement multi-factor authentication for external remote access by the end of October 2023.

The PHSA is in the process of reviewing technical and operational workflow requirements to ensure any changes to introduce multi-factor authentication are introduced with full consideration of the potential impacts on clinical workflows, patient care, and health information needs. As part of the series of consultations referenced in Recommendation 6, the PHSA will also collect information from participating organizations about their technical and operational workflow requirements to ensure a comprehensive assessment can be completed.

Multi-factor authentication is a primary tool in preventing compromised user credentials or internal misuse without accountability. The OIPC acknowledges that implementing multi-factor authentication is challenging, especially in a critical care environment where access to information is essential to successful outcomes. It is in this environment that having the System made unavailable due to a compromised user account is unacceptable.

The PHSA's completed Identity Risk Assessment is thorough and properly identifies the identity assurance requirements, as per the applicable provincial standards. There are numerous risk and control variables that may impact the decision respecting the necessary assurance level. A Security Threat and Risk Assessment (STRA) can identify and articulate risks associated with identity controls, such as the current threat environment for health information systems, how those attacks are perpetrated, and what controls are in place to prevent a successful attack. Based on the findings of the Identity Risk Assessment, the PHSA should ensure that all organizations accessing the System use multi-factor authentication.

The OIPC is encouraged that the PHSA is exercising appropriate due diligence while continuing to evaluate options for multi-factor authentication. The PHSA's completed risk assessment will also support in determining the most appropriate risk management solution.

The PHSA will provide the OIPC with a status update on progress related to implementing multi-factor authentication for all access to the System in January 2024.

Conclusion

The Provincial Public Health Information System collects significant volumes of sensitive personal information of all British Columbians relating to the delivery of health care and management of communicable disease outbreaks. Every day, hundreds of healthcare workers and policymakers across BC access the System. It is critical not only for the protection of British Columbians' information and privacy rights, but also for the continued delivery of essential services without disruption, that robust privacy and security controls be in place for the System.

The initial 2022 investigation found that given the volume and sensitivity of personal information in the System, the technical and security controls employed fell far short of what is reasonably necessary to protect the information and privacy rights of British Columbians.

The PHSA has taken positive steps to address the recommendations provided by the OIPC. Something as fundamental as a security architecture document will now provide the roadmap for implementing the security controls that should have been in place from the outset. Performing regular penetration testing will help identify the control areas that need strengthening, including user education.

The participating organizations who utilize the System are as diverse and complex as the services they provide across the province. While this may create additional challenges in meaningfully adopting security controls, the personal information maintained within the system is critical to the delivery of health services across the province. The consequences of not providing adequate protection have been catastrophic in other jurisdictions in Canada and abroad.[2] As a result, the level of protection required for the System must be commensurate with the nature, sensitivity, and criticality of the information.

The PHSA is to be commended for taking concrete steps to address the recommendations within the initial Investigation Report and we are confident it will continue using all means necessary to address outstanding issues. This will require commitment of resources and cooperation by all governance, management, and participating organizations. Implementing strengthened privacy and security controls will benefit all British Columbians, including the participating organizations tasked with delivering services through the System. The OIPC remains committed to following up with the PHSA until all recommendations are sufficiently addressed.

[2] For example, entire health care systems have been rendered unavailable and held for ransom, as was the case in the ransomware attack that impacted the Newfoundland and Labrador provincial health care system in 2021. See https://www.oipc.nl.ca/pdfs/P-2023-001-PH-2023-002.pdf, published May 23, 2023.

Public bodies and organizations not involved in this investigation are encouraged to read the original Investigation Report, along with the findings of this follow-up report. Investigations such as this one provide learning opportunities not only for the public body involved but for other public bodies and organizations, to help them understand their obligations for protecting personal information in a digital world.

Acknowledgements

I thank the President and Chief Executive Officer of the PHSA, Dr. David W. Byres, as well as all employees of the PHSA who contributed to this follow-up review by providing updates on the implementation of the recommendations, along with relevant documents and materials. I commend the PHSA for continuing to take positive steps toward fully addressing the recommendations.

All of us share a recognition of the System's importance to British Columbians. An ongoing commitment of resources to ensure the backbone of British Columbia's health system is properly secure and protected.

I would also like to thank Quinton Green, Senior Policy Analyst, and Tanya Allen, Director of Audit and Systemic Reviews, for conducting this investigation report follow-up and drafting this report with the assistance of security consultant Ken Prosser.

September 13, 2023

ORIGINAL SIGNED BY

Michael McEvoy
Information and Privacy Commissioner
for British Columbia