OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

OVERVIEW

LEFT UNTREATED: SECURITY GAPS IN BC'S PUBLIC HEALTH DATABASE

Background

The OIPC conducts audits, investigations, and compliance reviews to assess how effectively public bodies and private sector organizations protect personal information and comply with provisions under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA).

The System is a province-wide information service shared with the Yukon that supports public health programs such as immunization, communicable disease and outbreak management and family health programs such as maternal child health, early child health and family sexual health. The System is accessed by hundreds of healthcare providers who deliver these services, conduct surveillance activities and perform program evaluation.

The OIPC started the review in February 2022 due to several outstanding questions and concerns regarding the System's privacy and security protections.

Why?

The System, as it is referred to in the report, contains personal information about each of us – from personal health numbers to immunization records. If you have received medical care in BC for a pregnancy, a mental health issue, or for a sexually transmitted infection, you will find that sensitive personal information recorded in the System. And every day, thousands of healthcare workers and policymakers across BC access this System.

The System is indispensable when it is used for its intended purposes, which are the delivery of healthcare and managing threats like infectious disease outbreaks. However the System is subject to abuse, if wrongly accessed by any bad actor ranging from cyber criminals to a jilted lover looking for information about an ex to someone simply curious about their neighbour. Given its high level of sensitivity and the risk of its unauthorized access, the OIPC wanted to ensure that the highest degree of privacy and security is in place to protect personal information from such intrusions.

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

OVERVIEW

LEFT UNTREATED: SECURITY GAPS IN BC'S PUBLIC HEALTH DATABASE

What we found

No proactive patient privacy auditing	*Recommendation*: The PHSA should take immediate steps to 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.
No comprehensive security architecture	*Recommendation*: The PHSA should 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. The architecture should be signed and approved by senior officials at the PHSA and form the basis for an annual security audit.
No ongoing application vulnerability management program	*Recommendation*: The PHSA should immediately implement an ongoing application vulnerability management program to monitor for risk exposures related to unpatched software, and regularly report those to senior management.
No encryption of personal information within database	*Recommendation*: The PHSA should evaluate implementing the encryption of personal information within the Database.
No regular penetration testing	*Recommendation*: The PHSA should 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.

continued on next page

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

OVERVIEW

LEFT UNTREATED: SECURITY GAPS IN BC'S PUBLIC HEALTH DATABASE

continued from previous page

Vulnerable desktop environments

Recommendation: The PHSA should 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.

Multi-factor authentication not required for all users

Recommendation: The PHSA should 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.

"The System contains some of our most sensitive health information – matters relating to our mental and sexual health, infectious diseases, and more. It is imperative that the PHSA put in place commensurate security measures to protect British Columbians from potential harms." - Commissioner Michael McEvoy

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA