INVESTIGATION REPORT 22-02

Left untreated:
Security gaps in BC's public health database

DECEMBER 2022
CANLII CITE: 2022 BCIPC 73
QUICKLAW CITE: [2022] B.C.I.P.C.D. NO. 73

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

The Provincial Public Health Information System, or the System, as it is referred to in this report, contains personal information about almost all 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, hundreds of healthcare workers and policymakers across BC access this System, as they must.

The System is indispensable when it is used for its intended purposes, which are the delivery of healthcare and managing threats like communicable 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, one would expect the highest degree of privacy and security would be in place to protect our personal information from such intrusions.

But as we learned during our investigation, this is not so. There are many areas where the System is vulnerable. Its "entry gate" is weak. Multi-factor authentication is the industry standard for securing personal information, however it is not universally required for System access. Very disturbingly, there exists no proactive audit program that would alert authorities to those who try to use the System for nefarious purposes. Neither a malicious attack nor an authorized employee abusing their credentials is likely to be caught in the act.

It is troubling that the Provincial Health Services Authority (the PHSA), charged with responsibility for managing the System, has known about these risks since at least 2019, and has made little progress to address them.

Technical solutions for these System gaps exist, and they will cost money. The importance of bolstering our health care system's cybersecurity and privacy protections may not, at first glance, be as easily recognized as the value of adding more hospital beds, doctors, or shortening surgery wait times. But the consequences of failing to invest in privacy and security can be catastrophic. That is precisely how the New York Times described a recent breach of a database in Newfoundland and Labrador that effectively paralyzed the province's entire health care system.[1] These impacts are serious, and we need to treat them seriously.

I want to express my thanks to the most recently appointed President and Chief Executive Officer of the PHSA, Dr. David W. Byres. He assured me at the outset that my staff would have access to the information needed to do their work, and he made good on that commitment. He

[1] See "As Hackers Take Down Newfoundland's Health Care System, Silence Descends" Published Nov. 12, 2021, Updated Nov. 16, 2021, by Ian Austen: https://www.nytimes.com/2021/11/12/world/canada/newfoundland-cyberattack.html.

also assured me of his openness and desire to tackle the challenges that might be associated with my office's work. I also wish to thank the many PHSA staff members who provided documents and information necessary to complete this report.

I would also like to recognize Director of Policy Caitlin Lemiski, who led this investigation with the assistance of security consultant Ken Prosser.

All of us share a recognition of the System's importance to British Columbians. What is now required is the commitment of resources to ensure the very backbone of our health system is properly secured and protected for all of us.

Michael McEvoy
Information and Privacy Commissioner for BC
December 15, 2022

EXECUTIVE SUMMARY

The Provincial Public Health Information System, referred to in this report as the "System", collects personal information about all British Columbians to facilitate the delivery of healthcare and to manage outbreaks of communicable diseases. That personal information includes all manner of interactions with the System from vaccination status to mental health evaluations to a record of sexually transmitted infections. It should go without saying that the nature of this personal information is amongst the most sensitive and voluminous data held about us by any public body.

The entity charged with operating the System, also known as Panorama, is the Provincial Health Services Authority, or PHSA.

The Commissioner initiated this review following the PHSA's failure to provide satisfactory answers to questions about the System's privacy and security protections.

To conduct the investigation, the OIPC reviewed documents related to the technological controls PHSA has in place to protect personal information, and interviewed PHSA staff to determine whether the PHSA is properly protecting the personal information in the System Database.

This report finds that given the volume and sensitivity of personal information in the System, those protections fall far short of what is necessary to protect the public.

The investigation revealed that the PHSA's audit procedure for detecting malicious attacks and inappropriate use of the System is *reactive only,* generating reports for manual review *after events occur*. Investigators found the PHSA has no comprehensive security architecture documentation that would effectively guide its mitigation of security and privacy risks. While the PHSA undertook a major system upgrade to address outdated and unsupported software during the investigation, the OIPC learned the PHSA does not conduct regular penetration testing on the System that would disclose security vulnerabilities. Investigators discovered that the PHSA does not check to see that all desktop environments that are required to protect themselves from attack actually do so, leaving the entire System vulnerable.

Every British Columbian should be troubled by these findings, because it means personal information in the System is vulnerable to misuse and attack.

This report makes seven recommendations to the PHSA about how the System's privacy and security risks can be addressed.

1 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).[2]

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.

FIPPA provides that the Commissioner is "responsible for monitoring how this Act is administered to ensure that its purposes are achieved."[3] I decided to take a deeper look at the System when several of my questions and concerns regarding the System's privacy and security protections were not addressed.

Section 42(1)(a) of FIPPA gives me the authority to conduct audits and investigations to ensure compliance with that Act, and to gather evidence for either purpose, which has been done here. On February 9, 2022, I notified the PHSA of my office's intention to exercise my authority under s. 42(1)(a) to assess and make recommendations about the privacy and security of the System, and to share my report publicly.

To conduct this investigation, my office reviewed documents related to the technological controls the PHSA has in place to protect personal information and interviewed PHSA staff to determine whether the PHSA has practices in place to adequately protect the personal information in the System.

2 LEGISLATION

The purposes of FIPPA are to make public bodies more accountable to the public and to protect personal privacy.

The PHSA is a public body and is subject to FIPPA's security obligations. Section 30 of FIPPA contains the following requirement:

> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal.

[2] FIPPA, s. 42(1)(a) and PIPA, s. 36(1)(a).
[3] FIPPA, s. 42(1).

OIPC orders have established the meaning of "reasonable security arrangements." In short, for public bodies to meet their legislative obligations, they must take measures that are "objectively diligent and prudent in all of the circumstances."[4] Further, "the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure are factors to be taken into account in assessing the reasonableness of security arrangements."[5] As much of the personal information in the System is highly sensitive, the standard to protect that information is high.

3 OVERVIEW OF THE SYSTEM

In this section of the report, we set out the context in which the System operates and describe its history and structure.

3.1 Healthcare services in British Columbia

The provision of healthcare services in Canada is a shared responsibility between the federal and provincial governments.[6] In British Columbia (BC), there is a constellation of public bodies and organizations funded by the provincial Ministry of Health (the Ministry) that collectively makes up our healthcare system, including five regional health authorities: Vancouver Coastal Health, Fraser Health, Island Health, Interior Health, and Northern Health.[7] Two additional health authorities provide services province-wide: the First Nations Health Authority (FNHA)[8] and the PHSA.[9]

While each of these public bodies and organizations are separate entities, they must work together to provide coordinated health services throughout the province. This is where the System, also known as Panorama, plays a central role.[10] The PHSA operates the System for the benefit of all the other health authorities by maintaining a large database of health information. Ministry officials also access the System to conduct public health surveillance of communicable diseases like COVID-19. There are approximately four thousand individuals with access to the

[4] See "Sale of Provincial Government Computer Tapes Containing Personal Information, Re, 2006 CanLII 13536 (BC IPC)," https://canlii.ca/t/1n468, at paragraph 49.
[5] See https://www.oipc.bc.ca/special-reports/1271 at page 110.
[6] See: "Privacy and the USA Patriot Act" Implications for British Columbia Public Sector Outsourcing, October 2004: https://www.canada.ca/en/intergovernmental-affairs/services/federation/distribution-legislative-powers.html.
[7] See: BC Government website, "Regional health authorities", https://www2.gov.bc.ca/gov/content/health/about-bc-s-health-care-system/partners/health-authorities/regional-health-authorities.
[8] See: https://www2.gov.bc.ca/gov/content/health/about-bc-s-health-care-system/partners/health-authorities/first-nations-health-authority .
[9] The System also provides access to clinics called First Nations Health Service Organizations (FNHSOs) who hold agreements with the FNHA. The FNHA and every FNHSO are subject to BC's PIPA not FIPPA.
[10] See for example, "An Audit of the Panorama Public IT System" https://www.bcauditor.com/pubs/2015/audit-panorama-public-health-it-system.

System across hundreds of locations. The System Database holds entries on just over six million individuals.[11]

3.2 Origins

In the early 2000s, a global outbreak of Severe Acute Respiratory Syndrome (SARS) corresponded with significant advances in networking technology. In Canada, all levels of government came together to support an effort to develop modern electronic health information systems that could quickly and accurately help public officials track the spread of communicable diseases. Today, the provinces of Saskatchewan, Manitoba, Ontario, Quebec, New Brunswick, and Nova Scotia all maintain their own versions of the System. BC's version of the System was built by IBM Canada under a 2006 contract with the Ministry.[12]

3.3 The PHSA

The PHSA is responsible for the governance and management of the System under the terms of a 2016 Master Services Agreement.

The PHSA operates under the auspices of a Board appointed by the Ministry. The PHSA's Board receives its mandate from the Minister of Health. Most recently, on June 21, 2018, the Honourable Adrian Dix, Minister of Health, presented the Board with a multi-year foundational mandate letter[13] that assigns the PHSA responsibility for the digital information systems that support healthcare in BC. To fulfil this responsibility, Minister Dix directed the Board to ensure the PHSA works collaboratively with other public bodies and organizations. It is in this wider provincial context that the PHSA operates the System in accordance with the terms of the Master Services Agreement.

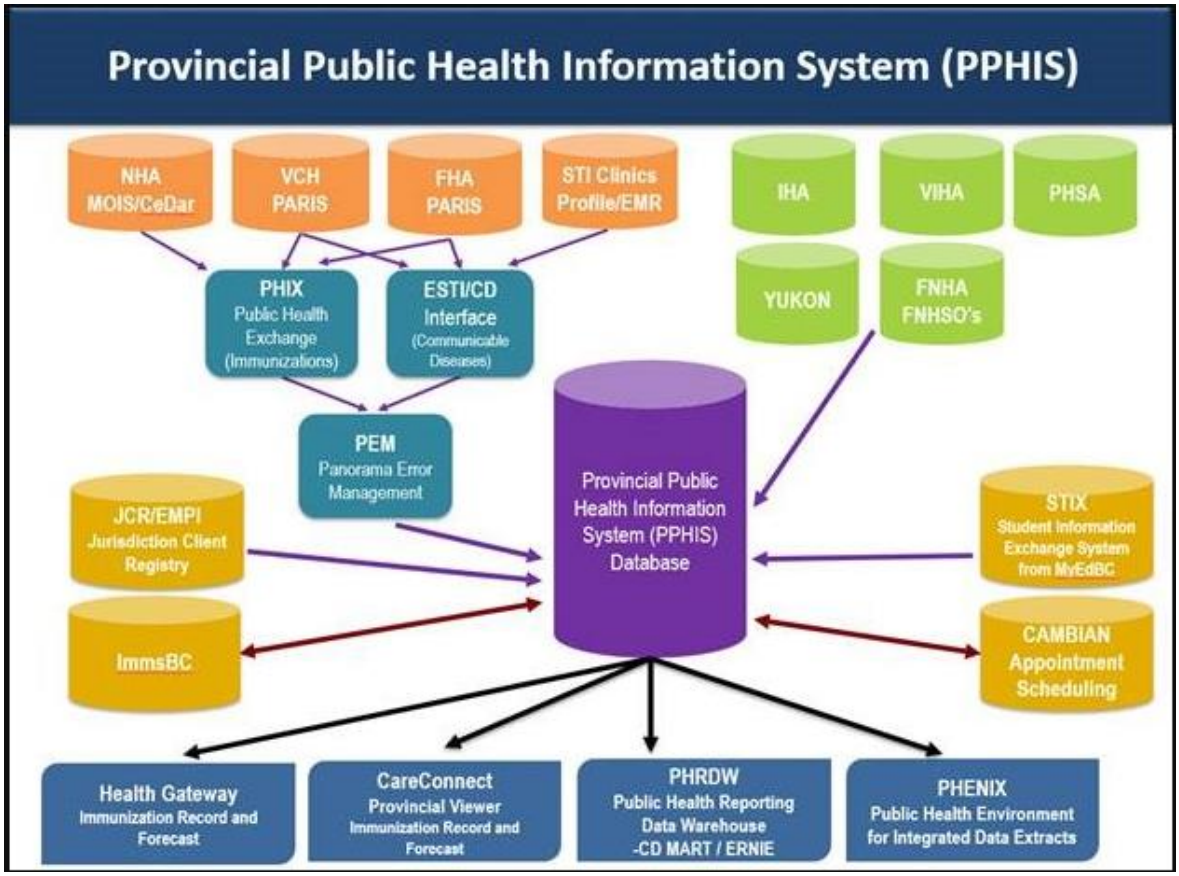
3.4 System structure

The central feature of the System is the System Database (see the purple cylinder in the diagram below). It supplies information to multiple entities and receives information from other ones, as indicated by the directional arrows in the diagram below.

[11] This data includes, but is not limited to, residents of BC and the Yukon, temporary foreign workers, as well as some deceased individuals.

[12] See "Pan-Canadian Public Health Communicable Disease Surveillance and Management Project Solution Integration Phase ASD Project Summary: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/about-the-bc-government/strategic-partnerships/the-strategic-partnerships-office/high-value-service-contracts/pchs_project_summary.pdf.

[13] See http://www.phsa.ca/about-site/Documents/PHSA%20Foundational%20%20Mandate.pdf. The Minister also issues annual mandate letters to the PHSA, available online at: Our Mandate (phsa.ca).



Source: PHSA website[14]

The result is a coordinated exchange of health information across different digital information services. For example, ImmsBC (in yellow) is an application that healthcare workers use to record an individual's COVID-19 vaccine or flu shot. In less than 24 hours, ImmsBC sends a copy of that vaccination record to the System Database. Once that information is in the System Database, other individuals can use other applications to access it. One of these is Health Gateway (in blue) that displays an individual's vaccination information on demand directly to their computer or smartphone.

3.5 System information

The System Database holds a vast amount of personal information. The amount held about any one British Columbian will of course vary depending on how long they have lived in the province and what health services they have received. The collection of information starts at birth, with the System Database storing the results of a variety of newborn health screening tests.[15] The data collection continues as an individual matures. For example, there are fields in the System Database for recording childhood vaccinations.

[14] See http://www.phsa.ca/health-professionals-site/PPHIS-Reference-Materials/PPHIS%20diagram.jpg.
[15] See: http://www.phsa.ca/health-professionals-site/PPHIS-Reference-Materials/Family-Health-Panorama/Downtime-Forms/Newborn-Assessment-Downtime-Form.pdf ; http://www.phsa.ca/health-

As an individual reaches sexual maturity, if they have sought healthcare related to a pregnancy, a sexually transmitted infection, or if they have completed a sexual health assessment[16] with a healthcare worker, the System Database has entry fields to record what that individual disclosed about how many sexual partners that individual has had, what sexually transmitted infections they have contracted, what types of sexual activity they have engaged in, and for women, how many pregnancies they have had and the outcome of each of those pregnancies.[17]

Additionally, if an individual has received one of many other kinds of assessments from a healthcare worker, there are fields in the System Database for recording information about an individual's mental health, their approximate income, as well as lifestyle habits like alcohol, tobacco and drug use, exercise, diet, and education level.[18]

Some of the data fields are very specific. For example, an HIV Case Report Form has fields to record whether an individual is a sex worker, whether they are using recreational drugs and which drugs they are using (there is a list of recreational drugs with tick boxes next to them), and how the individual is ingesting those drugs (for example the choices are oral, nasal, inhalation, injection and rectal).[19] The System Database also collects the contact information, worksite location information, international address and vaccination information of individuals temporarily living and working in BC as migrant workers.[20] In summary, there is an enormous volume of sensitive personal information that, if breached, could cause a significant list of harms including embarrassment, loss of dignity, family breakdowns, and even physical harm to individuals if it was accessed improperly.[21]

---

professionals-site/PPHIS-Reference-Materials/Family-Health-Panorama/Downtime-Forms/Dental-Assessment-Baby-Toddler-Downtime-Form.pdf.

[16] See: http://www.phsa.ca/health-professionals-site/PPHIS-Reference-Materials/Family-Health-Panorama/Downtime-Forms/Sexual-Health-Assessment-Downtime-Form.pdf

[17] See http://www.phsa.ca/health-professionals-site/PPHIS-Reference-Materials/Family-Health-Panorama/Standards-and-Guidelines/Provincial-Data-Definitions-and-Standards-for-Family-Health-v18.xlsx.

[18] *Ibid.*

[19] See: http://www.bccdc.ca/resource-gallery/Documents/Guidelines%20and%20Forms/Guidelines%20and%20Manuals/STI/HIVsurveillanceCRF_Oct2020-FINAL.pdf.

[20] See page 22: http://www.phsa.ca/health-professionals-site/PPHIS-Reference-Materials/COVID-19/Immunization-eForm-Guide.pdf If the migrant worker does not yet have a PHN (Personal Health Number) then this PDF instructs healthcare workers to record their temporary SIN number, passport number, or working visa number instead. According to the form, this information is supposed to be deleted from their file once they receive a PHN.

[21] For more examples of the personal information contained in the Database System, see "Surveillance of Reportable Conditions" at: http://www.bccdc.ca/health-professionals/clinical-resources/communicable-disease-control-manual/surveillance-of-reportable-conditions.

4 FINDINGS & RECOMMENDATIONS

To conduct this investigation, my office reviewed documents related to the technological controls the PHSA has in place to protect the System's personal information, and interviewed PHSA staff to determine whether their practices adequately protect personal information in the System Database. What follows are the conclusions drawn from those enquiries.

4.1 No proactive patient privacy auditing

Every day, thousands of individuals use the System to input and access personal information. The System logs each time someone accesses it. The public trusts that each access is for legitimate purposes. But we know that is not always the case. There are too many headlines about breaches involving identify theft, ransomware or someone with authorized credentials using their access to look up information about their neighbor, their former lover, or to acquire information for organized crime. These latter breaches are sometimes referred to as "snooping", but this grossly trivializes the violation of a person's privacy.

To address these privacy and security threats, the PHSA should be using adequate human and technological resources to prevent, detect and investigate suspicious behaviour. There is far too much activity happening on a daily basis within the System for humans alone to properly oversee all of it without the aid of technology. This is why implementing Security Information and Event Management (or SIEM, pronounced 'SIM') is essential.[22] SIEM is technology that helps to protect privacy by automating certain functions. Many of us have already experienced the power of SIEM when we log into an online account from a new device or location: our online account will text or email us an alert of the activity and instruct us to notify security if it was not us who logged on.

By design, SIEM is not an out-of-the box solution; it is a sophisticated tool that must be customized to fit the environment in which it is being deployed. Correctly configured, a privacy-tailored SIEM can generate a variety of useful alerts of suspicious activity. For example, SIEM can generate an alert if an employee is looking up individuals living on the same block as them or with the same last name as them. SIEM can also generate alerts if a large volume of information is being exported from a database, signaling a potential cyberattack.

To be effective, a SIEM-generated alert is only valuable if there is a qualified human being on the other end of the alert who can respond to it. This means that organizations must adequately staff their security and privacy departments to properly support SIEM maintenance and privacy investigations.

---

[22] For more, see this website and video from BC Government: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security/security-respiratory-controls/logging-and-monitoring. Also see the NIST's Computer Security Resource Centre's entry for "SIEM" online at: https://csrc.nist.gov/glossary/term/security_information_and_event_management_tool.

Given how sensitive the personal information in the System is, we would expect the PHSA to have a privacy-tailored SIEM in place. Indeed, the System's audit policy makes numerous references to proactive auditing.[23] However, our investigation revealed that the PHSA had implemented an audit tool that is *reactive only,* generating reports for manual review *after events occur*. Without SIEM and adequate human resources to support proactive monitoring and investigation, suspicious activity will go undetected or responded to unless someone has complained. If no one has complained, then privacy breaches may succeed with no accountability to the patients who have had their personal privacy intruded upon. The PHSA acknowledges that its current auditing tool is inadequate and that it is looking for a new solution capable of proactive audits.

In addition to meeting its responsibilities to protect personal information under s. 30 of FIPPA, a comprehensive, privacy-tailored SIEM may also protect against civil liability. In August 2022, Justice Smith of the BC Supreme Court held that BC's public auto insurer, the Insurance Corporation of BC (ICBC), was vicariously liable for the actions of one of its employees who improperly accessed addresses associated with certain licence plates and sold them to a third party.[24] Many of those addresses were later subject to arson or firearms attacks. In finding ICBC vicariously liable, the Justice reasoned that ICBC foresaw that employees might ignore rules and policies designed to prevent employees from improper use of its databases, but that there was "no evidence of any system or method that would have prevented or detected that conduct at the time it happened."[25] Based on our review, the PHSA is in a comparable situation with respect to the System Database.

RECOMMENDATION 1

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.

4.2 No comprehensive security architecture

Houses need blueprints. Pilots need flight plans. And system security administrators need security architecture. Security architecture is a documentation of the security controls that must be implemented to meet system security requirements based on regulatory requirements, contractual obligations, and risk analysis. This documentation is a technical interpretation of policies and standards, and is used in the systems design process, operations

[23] See "Panorama Access Audit Policy" (lasted updated February 2018).
[24] *Ari v Insurance Corporation of British Columbia*, 2022 BCSC 1475 (CanLII), <https://canlii.ca/t/jrlhv>.
[25] *Ibid* at para. 75.

guides, user manuals, and other materials to ensure that a system is secure and that it meets an organization's business objectives. In the case of the System, for example, comprehensive security architecture would tell employees to use SIEM and how to configure it to help protect patient privacy and support privacy investigations. It would also allow outsiders like this office to evaluate whether the PHSA is meeting its security requirements.

From a legal perspective, security architecture is also valuable. It details what an organization's risk tolerance is and how to address privacy and security challenges. Without it, for example, systems developers and operations staff have nothing to guide the implementation and configuration of controls and generally what the ongoing operational requirements of a system should be. At best, it will result in an attempt to implement controls that meet policy and standards; at worst, it will mean implementation in an ad hoc manner, or not at all if they are seen to be too costly or complicated.

When we asked the PHSA for its security architecture for the System we were provided with a Security Threat and Risk Assessment that it completed in 2019. The PHSA informed us that they used this STRA as documentation of the security architecture, and has other documentation across various areas of responsibility that also address security architecture. A STRA is a documented evaluation process to detect and assess risks to an information system, and recommend strategies to mitigate them.[26] A STRA is *not* security architecture. While the 2019 STRA has a very descriptive section about the System Architecture, and a good analysis of whether security controls are effectively mitigating risk, it is primarily a point-in-time assessment of the System's security risk. What the 2019 STRA did tell us is that the PHSA has known about the privacy and security risks documented in this report since at least 2019, and despite their seriousness, the PHSA has not put in place proper security architecture documentation that would effectively guide the PHSA's mitigation of risks.

RECOMMENDATION 2

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.

[26] For more on STRAs, see: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology.

4.3 No ongoing application vulnerability management program

The System is supported by several computer programs supplied by a number of companies. Taken together, the programs, written in computer language or code, allow the System to operate. At the same time, the programs and underlying codes pose an inherent serious privacy and security risk. Just like English is a living language, computer code is a language living at the speed of light: certain lines of code can quickly become outdated, nonsensical, or even harmful to a system. Computer code can also be secretly modified to do everything from making a webpage load slowly to damaging nuclear facilities.[27] The well-known "SolarWinds" cybersecurity incident is a recent example of this.[28]

To mitigate these risks, an organization's security professionals must frequently review and test their program code. Program code may be acceptable one week, but unacceptable the next if a vulnerability is discovered that could be exploited to gain unauthorized access to a system. Therefore, remediating the code, also known as "patching", is critically important.

Not patching is like leaving your front door unlocked, waiting for an unscrupulous person to take advantage.

Code developers will send their clients specific patches, or will bundle several patches into a major software update or new version for clients to review and install to ensure their system remains robust and up to date. Sometimes however, the original authors of the code announce they will no longer provide support (send patches), for older versions, or the company that makes the software goes out of business. When this happens, security professionals must remove the "unsupported" code and replace it with "supported" code that still receives patches, or develop a risk mitigation strategy that allows the safe use of the unsupported software.

The 2019 STRA identified several of the System's components that deployed software with code that was either unpatched or no longer supported. The STRA assessed the privacy and security risk of not patching the code or removing unsupported code as "high." During the course of our investigation, the PHSA undertook a major system upgrade to address outdated and unsupported software, and performed vulnerability assessments and penetration testing to identify security risks that could lead to a privacy breach. It is incumbent upon the PHSA to undertake this work on an ongoing basis. This means the PHSA must implement an ongoing application vulnerability management program to address present and future risks.

---

[27] See, for example "Timeline of computer viruses and worms", Wikipedia: https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms and Stuxnet https://en.wikipedia.org/wiki/Stuxnet.

[28] For more, see the US Government Accountability Office's report: https://www.gao.gov/products/gao-22-104746.

RECOMMENDATION 3

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.

4.4 No encryption of personal information within database

When data is transferred across the internet it is most often encrypted or scrambled to protect against someone reading it in the event it is intercepted. When the data arrives at its intended destination, it is said to be data "at rest." This data could include personal information, and for this reason it is often important for data at rest to be encrypted. A good example frequently encountered by consumers is the "save credit card information" option offered when you make an online purchase. That credit card information will be stored in a database with thousands of other credit card numbers. If the company managing those credit card entries does not encrypt this personal information at rest, it will be in plain sight to anyone accessing the database, from the database administrator in charge of it to a possible hacker who gains unauthorized entry. If the credit card entries are properly encrypted, it makes it extremely difficult to understand or make any use of the data.

With respect to the System Database, we learned that the disks the Database files are stored on, and their associated backup files, are encrypted. This prevents any privacy breach if the physical disks are ever stolen or improperly disposed of. However, the Database files on the disks themselves containing the personal information are not encrypted and become accessible to authorized users once the application is started. Database encryption allows for a further level of access control and is considered industry best practice when protecting personal information. The PHSA should evaluate what steps can be taken to add a further level of encryption within the Database to increase protection of the most sensitive personal information.

RECOMMENDATION 4

The PHSA should evaluate implementing the encryption of personal information within the Database.

4.5 No regular penetration testing

Penetration testing (or simply "pen testing"), is designed to test the robustness of a system's privacy and security protections. In most cases the head of an organization's security will hire an outside expert to try to gain access to its system. Penetration testing is sometimes called "white hat hacking" or "ethical hacking".[29] Often, the head of security will not warn that a pen test is going to take place, because they want to see if the organization's people, in the ordinary course of events, are able to detect the attack. If the hired expert manages to access the System, the security experts can study how they got in, how long they were able to stay in, and what they were able to see and do when they were inside. In the physical world, an example of penetration testing is when airport security authorities test screening systems and personnel by placing banned items in luggage to see if they make it past those defences.

It is fundamental to ensure that a system's privacy and security protections are fit for purpose. While the PHSA conducted penetration testing after we launched our investigation, it has otherwise failed to do so on a regular basis.

Given the volume and sensitivity of the personal information in the System Database, and the number of individuals who have access to it, the PHSA should conduct annual penetration testing on the System and develop corresponding action plans that mitigate the risks they identify as a result. Performing this testing would also support the PHSA's compliance with its Master Services Agreement with the Ministry, which requires it.[30]

RECOMMENDATION 5

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.

4.6 Vulnerable desktop environments

In cybersecurity speak, a "threat vector" is anything that a bad actor can use to gain unauthorized access to a system. A "desktop environment" is what you see when you turn on your computer. Desktop environments are threat vectors. An analogy would be that a step stool is a threat vector to a child gaining access to candy in a cupboard. Hide the step stool in the closet, and you have just mitigated that risk.

[29] See the NIST glossary: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary.
[30] See the Agreement at p. 23, section 3.11(xii).

A likely way to attack the System Database is to gain access to a vulnerable desktop environment — and there are thousands of desktops that have access to the System. Some, managed by the PHSA and the regional health authorities, have deployed sophisticated computer programs on all their workstations, detecting and preventing malicious software or cyberattacks. This is a positive measure and a proper approach to risk mitigation. However, we do not know whether desktops outside the PHSA and regional health authorities that access the System are similarly managed.[31] My investigators learned that although the PHSA requires all desktop environments accessing the System to be adequately protected from an attack, it does not actually check to see whether that is so. A single vulnerable desktop puts the entire System Database at risk and for this reason the PHSA should properly secure desktops that connect to the System. Where a desktop cannot be secured the PHSA should provide those users with a single secure access portal (a virtual desktop environment for example) that can be monitored by the PHSA for compromise.

RECOMMENDATION 6

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.

4.7 Multi-factor authentication not required for all users

Anyone who needs access to the System to do their job must first prove who they are. Proving or authenticating yourself is key to a system's security, and the more authentication factors used in the process, the more secure the log-on. There are three authentication factors: something you know, something you have, and something you are. When someone types in a user name and password to authenticate themselves, they are using the same factor twice – something they know. Other people can steal that information or even guess it. Because of this, systems are much more secure when users must enter at least two factors to gain access. A common example is using a bank card with a personal identification number (PIN) – this is an example of something you know (the PIN) and something you have (the card).[32]

Multi-factor authentication (MFA) is important as it is the most effective way to prevent system breaches by hackers, and to ensure accountability for unauthorized user activity because it makes it much harder for someone to log on to a system as someone else. Pretend a thief has

[31] These include First Nations Health Service Organizations (FNHSOs). For more about FNHSOs, see footnote 11, *ibid.*

[32] See https://csrc.nist.gov/glossary/term/multi_factor_authentication; also see https://www.nist.gov/blogs/cybersecurity-insights/out-old-new-making-mfa-norm. Back to basics: Multi-factor authentication (MFA) | NIST.

stolen a user name and password to a system. If that system also requires a user to plug a token into their computer, then unless the thief also has the token, the thief's attempts will fail.

MFA is important for the System because it has so many users and because it contains such sensitive personal information. With thousands of users spread across both BC and the Yukon, the risk of a user's account being compromised by something like a phishing attack is very high.[33] The mandatory use of an MFA solution for all System accesses would go a long way to prevent a successful attack.

Our review found that the PHSA only requires MFA for remote access to the System. Access from health authority facilities and office locations, which comprise most of the users, does not require any form of MFA. Given the high level of sensitivity and volume of the personal information in the System Database, the PHSA should conduct an Identity Risk assessment to determine the appropriate level of Identity Assurance required.[34] The Province's Identity Assurance Standard, which should guide such an assessment, would suggest the System requires a High Assurance Level.[35] Achieving the High Assurance Level requires the use of MFA for ongoing system access.[36]

The Province has already established a high-assurance MFA solution for citizens' access to the System when they use Health Gateway.[37] It would no doubt represent a significant undertaking if the Province's Identity Assurance Standard points to fully implementing a High Assurance MFA solution for all users of the System. However, the consequences of not doing so would be potentially catastrophic as demonstrated in recent healthcare cyberattacks.[38]

---

[33] A "phishing" attack is when someone tries to trick someone into giving up their personal or sensitive information and/or by clicking on a link that will allow an attacker to access that information. For more, see the NIST Glossary under the entry for "Phishing" https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary.

[34] See: Identity Assurance Standard Section 3.1.1 at https://alpha.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/identity_assurance_standard.pdf.

[35] *Ibid* at section 2.2 "Identity Assurance Levels".

[36] *Ibid* at section 2.2 under "High Identity Assurance" which states "Identity claims are substantiated through the in-person presentation of evidence and require the individual to use a multi-factor credential for future transactions. This combination provides high confidence in the truth of the claim."

[37] See https://www.healthgateway.gov.bc.ca/.

[38] In addition to the cyber attack experienced by Newfoundland and Labrador's healthcare system mentioned earlier in this report, there have been other serious cyberattacks. For example, see "Cyber-attack on Irish health service 'catastrophic'" May 20, 2021 at https://www.bbc.com/news/world-europe-57184977 and "HSE cyber-attack: Irish health service still recovering months after hack" September 5, 2021 at https://www.bbc.com/news/world-europe-58413448. Also see "Pinnacle Health hack: Sensitive files posted to the dark web include 'confidential' report" October 9, 2022 at https://www.nzherald.co.nz/business/pinnacle-health-hack-sensitive-files-posted-to-the-dark-web-include-confidential-report/6FBTOGMJANQBSF2QAUE4ZVPHTE/.

RECOMMENDATION 7

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.

5 CONCLUSION

This report set out to determine whether the PHSA properly protects the personal information of British Columbians in the Provincial Public Health Information System. We found that they do not. Indeed, given the volume and sensitivity of the personal information in the System, those protections fall far short of what is necessary to protect the public.

What the public has a right to expect are robust security practices that include proactive monitoring of suspicious activity, securing all desktops with access to the System, and strong authentication processes. The PHSA has begun to address matters we have identified, and much critical work remains. What is at stake is the very trust British Columbians place in our health care system to protect the sensitive personal information it holds about all of us.

December 15, 2022

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

6 APPENDIX A: RECOMMENDATIONS

RECOMMENDATION 1: 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.

RECOMMENDATION 2: 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.

RECOMMENDATION 3: 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.

RECOMMENDATION 4: The PHSA should evaluate implementing the encryption of personal information within the Database.

RECOMMENDATION 5: 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.

RECOMMENDATION 6: 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.

RECOMMENDATION 7: 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.