Chapter 17
eHealth Saskatchewan—Securing Portable Computing Devices

1.0 Main Points

eHealth Saskatchewan is responsible for managing critical IT services used to administer and deliver healthcare services in Saskatchewan, which includes configuration and security of portable computing devices accessing the eHealth IT network. Portable computing devices (e.g., laptops, smartphones) create security risks because they may become infected with viruses or malware and are easy to lose.[1] As of August 2024, almost 32,000 portable computing devices can access the eHealth IT network.

By August 2024, eHealth made some progress toward securing portable computing devices, but it still needs to:

- Implement adequate configuration settings on all eHealth-managed laptop devices with access to the eHealth network
- Complete implementation of a central mobile device management system, which can help to reduce the risk of inconsistent configuration settings on mobile devices that expose the devices and the eHealth IT network to viruses and malware
- Sufficiently control and monitor access to the eHealth IT network to detect and prevent malicious activity to help mitigate the impact of security breaches

eHealth also needs to work with its health sector partners to improve its tracking of lost or stolen devices so eHealth can ensure it appropriately removes all portable devices from the network. Not properly wiping or removing portable devices from the eHealth IT network if lost or stolen increases the risk of unauthorized access to confidential health information on the device and the network.

2.0 Introduction

2.1 Background

eHealth Saskatchewan is responsible for managing critical IT services used to administer and deliver healthcare services in Saskatchewan. This includes responsibility for Saskatchewan's electronic health record and health information systems, and IT systems in use at the Saskatchewan Health Authority, Saskatchewan Cancer Agency, 3sHealth, and the Ministry of Health.[2]

[1] Malware is software specifically designed to disrupt, damage, or gain unauthorized access to computing devices.
[2] In January 2017, the Minister of Health directed eHealth to consolidate IT services into a single service that the Saskatchewan Health Authority, Saskatchewan Cancer Agency, and 3sHealth previously provided. eHealth also hosts IT systems used at the Ministry of Health.

Almost 32,000 portable computing devices can access the eHealth IT network.[3] Portable computing devices include devices such as smartphones and laptops.

As of August 2024, eHealth employed about 786 staff.[4] eHealth is responsible for the configuration and security settings applied to portable computing devices it manages. In addition, it is responsible for monitoring the security of the eHealth IT network housing critical IT health systems and data essential to the management and delivery of provincial health services along with a significant amount of other private and confidential data (e.g., provincial health card information).

2.2 Focus of Follow-Up Audit

This chapter describes our second follow-up audit of management's actions on the six recommendations we made in 2020.

We concluded eHealth Saskatchewan had effective processes, except in the areas identified in our seven recommendations, to secure health information on portable computing devices used in delivery of Saskatchewan health services from unauthorized access for the 12-month period ended August 31, 2019.[5] By June 2022, eHealth implemented one recommendation.[6,7]

To conduct this audit engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook—Assurance* (CSAE 3001). To evaluate eHealth's progress toward meeting our recommendations, we used the relevant criteria from the original audit. eHealth management agreed with the criteria in the original audit.

To complete this follow-up audit, we discussed actions taken with management. We reviewed policies related to portable device security (e.g., password policy, lost or stolen device policy) and examined network security logs and scans eHealth used to monitor its IT network. In addition, we used an external consultant to assess network access controls and system configuration for a sample of portable computing devices (i.e., laptops and smartphones) against good practice.

3.0 Status of Recommendations

This section sets out each recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of the recommendation at August 15, 2024, and eHealth Saskatchewan's actions up to that date.

[3] Information provided by eHealth Saskatchewan.
[4] Ibid.
[5] *2020 Report – Volume 1*, Chapter 6, pp. 47–63.
[6] *2022 Report – Volume 2*, Chapter 15, pp.175–182.
[7] In 2023, we followed up on two of the seven recommendations within our annual integrated audit of eHealth. By March 2023, eHealth had partially implemented the two recommendations about IT network access controls and monitoring. *2023 Report – Volume 2*, Chapter 1, pp. 13–18.

3.1 Laptop Configuration Still Includes Some Unaddressed Risks

We recommended eHealth Saskatchewan implement a written risk-informed plan to protect laptops with access to the eHealth IT network from security threats and vulnerabilities. *(2020 Report – Volume 1*, p. 56, Recommendation 2; Public Accounts Committee agreement January 12, 2022)

Status—Partially Implemented

eHealth Saskatchewan implemented its standard laptop configuration, including encryption, with almost all its laptops using a supported operating system as of August 2024. However, eHealth continued to permit unrestricted use of USB ports in laptops—it planned to implement a pilot program to mitigate these risks by March 2025. eHealth also needs to restrict the users' ability to access a laptop's BIOS settings.[8]

We found eHealth made progress in implementing its standard laptop configuration—at August 2024, about 99% of its laptops used a supported operating system (e.g., Windows 10) that includes encryption. Configuring laptops with supported operating systems and encryption helps to protect devices against known vulnerabilities and reduces the risk of compromise in the event a laptop is lost or stolen.

However, we also found eHealth's standard laptop configuration continued to permit unrestricted use of USB ports in laptops. eHealth plans to pilot restricted use of laptop USB ports at one agency by March 31, 2025, and expand to other agencies on the eHealth IT network after the pilot. Management indicated that as certain health sector partners use USB ports to deliver clinical services, eHealth needs to take a phased approach to restricting the use of USB ports to minimize service disruptions. Blocking the USB ports can prevent devices from downloading data or uploading malicious software or tools.

In addition, our review of the standard configuration found users continue to have access to the BIOS settings—permitting users to control device settings at the hardware level. At August 2024, eHealth decided to restrict access to BIOS settings and was working on a plan to implement this as a standard configuration setting. Access to BIOS settings allow users to change hardware configurations, increasing the risk of security vulnerabilities if they make unauthorized changes.

3.2 Central Mobile Device Management Coming

We recommended eHealth Saskatchewan standardize the configuration settings for mobile devices with access to the eHealth IT network to mitigate associated security threats and vulnerabilities. *(2020 Report – Volume 1*, p. 59, Recommendation 3; Public Accounts Committee agreement January 12, 2022)

Status—Partially Implemented

[8] BIOS (basic input/output system) is the program a computer's microprocessor uses to start the computer system after it is powered on. It also manages data flow between the computer's operating system and attached devices, such as the hard disk, video adapter, keyboard, mouse, and printer. BIOS security is a component of cybersecurity that organizations should manage to prevent hackers from executing malicious code on the operating system. techtarget.com/whatis/definition/BIOS-basic-input-output-system (16 October 2024).

We recommended eHealth Saskatchewan analyze the cost-benefits of use of a central mobile device management system to secure and monitor mobile devices with access to the eHealth IT network. *(2020 Report – Volume 1*, p. 59, Recommendation 4; Public Accounts Committee agreement January 12, 2022)

Status—Implemented

eHealth Saskatchewan selected a central mobile device management system to help secure and monitor mobile devices (e.g., smartphones). While eHealth appropriately configured the central device management system in accordance with good practice, eHealth has only transitioned 14% of its mobile devices to the central system—resulting in the configuration settings for many mobile devices not aligning with good practice in several areas (e.g., password requirements, blocking jailbroken or rooted devices, containerization).[9,10]

At August 2024, eHealth is responsible for almost 8,000 mobile devices. eHealth's configuration of mobile devices differs based on health sector agency (e.g., eHealth, Saskatchewan Health Authority) and location. Since 2019, eHealth uses three mobile-device management systems to manage mobile devices with access to the eHealth network. Since our last follow-up audit, eHealth selected one of these systems for implementation as its central system for all health sector agencies by 2025–26.

Fully implementing a central mobile device management system and requiring staff to register their mobile devices on that system can help ensure only authorized users have access to corporate emails, contacts, or calendars.

We tested eHealth's standard configuration settings for mobile devices and found:

- **Password settings do not align with good practice for most devices**. Good practice suggests mobile device passwords require six characters, restrict the use of sequential characters, and restrict the use of repetitive characters.

At August 2024, eHealth's policy requires a password to be at least six characters in length and prohibits the use of sequential and repetitive characters (e.g., 000000), which aligns with good practice. However, eHealth only enforces this policy on one of its three mobile-device management systems for 14% of the mobile devices eHealth manages. Password requirements not in alignment with good practice increase the risk of compromised mobile devices.

- **Not all jailbroken/rooted devices blocked**. Good practice suggests blocking the use of jailbroken/rooted devices for corporate usage as staff may use these devices to bypass manufacturer restrictions and security protections, exposing the device and the eHealth IT network to vulnerabilities.

[9] Jail Break/Rooting: Bypassing the restrictions placed on the mobile device by the manufacturer. With a jailbroken mobile device, users can install apps and change settings not authorized by the manufacturer. Additionally, it removes the default security protections built into the mobile device by the manufacturer.

[10] Containerization creates a secure and segregated user profile from the staff's personal profile. This approach isolates applications and data specific to the organization from the staff's personal applications and data.

- **Containerization not consistently used**. Good practice suggests the use of containerization to separate personal usage of mobile devices from corporate usage. Lack of containerization increases the risk of attack from personal use of mobile devices.

- **Not all devices restrict application downloads**. Good practice suggests restricting downloads on mobile devices to only corporate-approved applications and stores.

At August 2024, eHealth configured two of its three mobile-device management systems to restrict jailbroken and rooted devices on the eHealth IT network, application downloads, and to segregate corporate and personal applications and data. However, we found these restrictions only applied to 46% of the mobile devices that eHealth manages.

eHealth indicated it plans to transition all mobile devices to its central mobile device manager by March 31, 2026.

Inconsistent configuration settings on mobile devices result in increased security risks. Well-configured security settings can protect the eHealth IT network from malicious software by limiting what users can access on their mobile devices through containerization, and applying restrictions on applications.

3.3 Need to Centralize Incident Management and Track All Lost or Stolen Portable Devices

We recommended eHealth Saskatchewan take appropriate action to minimize the risk of security breaches when a portable computing device is reported lost or stolen. *(2020 Report – Volume 1*, p. 60, Recommendation 5; Public Accounts Committee agreement January 12, 2022)

Status—Partially Implemented

eHealth Saskatchewan implemented a process to centrally track lost or stolen portable computing devices with access to the eHealth IT network, but we found eHealth's tracking spreadsheet incomplete as it did not include all lost or stolen devices. In addition, eHealth has yet to adopt a centralized incident management process for all devices accessing its IT network.

eHealth uses information from its ticketing system to manually update a spreadsheet about lost or stolen devices. Between January 2023 and August 2024, we found eHealth recorded 12 incidents that resulted in 18 lost or stolen devices.

Using information obtained from the Saskatchewan Health Authority, we found six additional lost or stolen devices managed by eHealth not included in its tracking spreadsheet. While we tested two of these devices and found eHealth appropriately disabled the devices and removed them from the network, eHealth may not know the full extent of lost or stolen portable computing devices at the health sector agencies to which it provides services.

Additionally, we found eHealth does not have a centralized incident management process for all devices accessing its IT network. It does not have authorization to disable all of the Authority's mobile devices for Saskatoon and surrounding area (i.e., the Authority has almost 2,400 mobile devices in Saskatoon)—these device owners must contact their cell phone provider to disable lost or stolen devices. eHealth is responsible for taking appropriate action to minimize the risk of security breaches by removing a device from the network, disabling a device, and wiping a device, if applicable. eHealth indicated it is working with the Authority to obtain authorization to disable these devices when necessary to do so—it expects to obtain such authorization by March 31, 2026.

Not having complete information about lost or stolen devices, or a centralized incident management process, increases the risk of lost or stolen portable computing devices not being appropriately removed from the network and those devices being compromised, putting personal health information at risk.

3.4 Enhanced Network Access Controls Still Needed

We recommended eHealth Saskatchewan implement a risk-based plan for controlling network access to mitigate the impact of security breaches.

(2020 Report – Volume 1, p. 61, Recommendation 6; Public Accounts Committee agreement January 12, 2022)

Status—Partially Implemented

eHealth Saskatchewan needs to implement its plan to control network access.

eHealth is working toward centralized controls for network access for all health sector agencies and network access ports.[11] eHealth planned to pilot network access controls in one medium and one large healthcare facility (e.g., hospitals) by March 31, 2023, but paused the pilot project in August 2023 to focus its efforts on data centre network controls.

eHealth indicated it is developing a plan for establishing network access controls for all health sector agencies.

Without network access controls, eHealth does not sufficiently control access to the eHealth IT network, and it does not restrict where users and devices can go on or what they can do on the eHealth IT network.

Establishing IT network access controls to restrict user access to only what they need at any given time makes it much harder for attackers to escalate privileges and take aim at vital assets (in the event a portable device is compromised). Good practice also suggests the use of network segmentation to limit movement across a network in the event an attacker gains unauthorized access to a network.

Without adequate security on network access ports, the eHealth IT network may be vulnerable to attack through these open ports. Controlling IT network access helps to mitigate the risk of security breaches, and the extent of breaches.

[11] Network Access Control (NAC) is the process of restricting unauthorized users and devices from gaining access to a corporate or private network. NAC ensures that only authenticated users and devices that are authorized and compliant with security policies can enter the network. fortinet.com/resources/cyberglossary/what-is-network-access-control (16 October 2024).

3.5 Progress on Network Access Monitoring

We recommended eHealth Saskatchewan utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity. *(2020 Report – Volume 1*, p. 62, Recommendation 7; Public Accounts Committee agreement January 12, 2022)

Status—Partially Implemented

eHealth Saskatchewan began using a service provider in May 2023 to help monitor and manage the security of its IT network; however, it has yet to transfer responsibility for monitoring all aspects of the network to service providers as planned.

eHealth continues to monitor pieces of the eHealth IT network, including endpoint protection and real-time scanning from key points in the eHealth network, but it does not scan all areas of the IT network and analyze results to detect malicious activity.

Service providers can bring additional tools needed to effectively detect, prevent, and control malicious activity on the eHealth IT network—such as extended detection and response solutions and 24/7 monitoring of the eHealth IT network.[12] At August 2024, eHealth had yet to transfer responsibility for monitoring all aspects of the network to service providers as planned.

Without effective IT network monitoring, eHealth may not detect malicious activity and mitigate risks of a successful attack on its corporate network within sufficient time to prevent a security breach.

[12] Extended detection and response collects and automatically correlates data across multiple security layers—email, endpoint, server, cloud workload, and network—allowing for faster detection of threats and improved investigation and response times through security analysis. trendmicro.com/en_in/what-is/xdr.html#:~:text=XDR%20(extended%20detection%20and%20response,XDR (16 October 2024).