Chapter 15
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 portable computing devices that access the eHealth IT network. Portable computing devices (e.g., laptops, smartphones) create security risks for organizations because they are attractive targets for attackers, may become infected with viruses or malware, and are easy to lose.[1]

By June 2022, eHealth implemented annual security awareness training for all portable computing device users and implemented a centralized system to manage and configure laptops. However, eHealth still needs to:

- Implement adequate configuration settings on all eHealth-managed portable computing devices with access to the eHealth network.

  Inappropriate security settings on portable computing devices can 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.

  Portable computing devices create paths to IT networks. Controlling and monitoring eHealth IT network access helps to mitigate the impact of security breaches.

- Work with its health sector partners to improve notification of all lost or stolen portable computing devices so it can appropriately wipe or remove the devices from the network.

  Not properly wiping mobile devices or removing laptops from the eHealth IT network if lost or stolen increases the risk of unauthorized access to confidential health information on the device and to 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

[1] Malware is software specifically designed to disrupt, damage or gain unauthorized access to computing devices.

in use at the Saskatchewan Health Authority, Saskatchewan Cancer Agency, 3sHealth, and the Ministry of Health.[2]

Almost 15,000 portable computing devices can access the eHealth IT network. Portable computing devices include smartphones, tablets, and laptops.

As of August 2022, eHealth had about 440 staff. Its technology program area is responsible for the configuration and security settings applied to portable computing devices. Its IT security team is responsible for monitoring the security of the eHealth IT network. This network houses 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 first follow-up audit of management's actions on the seven recommendations we first made in 2020.[3]

In 2019, we assessed eHealth Saskatchewan's processes to secure health information on portable computing devices used in delivery of Saskatchewan health services from unauthorized access. Our *2020 Report – Volume 1*, Chapter 6, concluded that eHealth had effective processes, other than the areas of our seven recommendations.[4]

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's management agreed with the criteria in the original audit.

To complete this follow-up audit, we discussed actions taken with management. We reviewed eHealth's annual security training program and associated monitoring. We also 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 the 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 June 15, 2022, and eHealth Saskatchewan's actions up to that date.

[2] In January 2017, the Minister of Health directed eHealth to consolidate IT services into a single service that the Authority, Saskatchewan Cancer Agency, and 3sHealth previously provided. eHealth also hosts IT systems used at the Ministry of Health.
[3] In 2021, we followed up on two of the seven recommendations within the annual integrated audit of eHealth. By March 2021, eHealth had partially implemented the two recommendations about IT network access controls and monitoring. *2021 Report – Volume 2*, Chapter 3, pp. 13–17.
[4] *2020 Report – Volume 1*, Chapter 6, pp 47-63.

3.1 Security Awareness Training Program Implemented

We recommended eHealth Saskatchewan work with the Saskatchewan Health Authority to implement an annual security awareness training program for users of portable computing devices with access to the eHealth IT network. *(2020 Report – Volume 1,* p. 53, Recommendation 1; Public Accounts Committee agreement January 12, 2022)

Status—Implemented

In 2021, eHealth Saskatchewan implemented an annual security awareness training program for all individuals accessing the eHealth IT network.

eHealth requires all users who can access the eHealth IT network to complete the security awareness training annually. Our review of the training program found it includes a module addressing mobile devices. The module provides users with information about mobile device security vulnerabilities and best practices for protection (e.g., strong passwords; encrypting sensitive, personal or confidential information in outgoing communication; deleting email and text messages from unknown senders).

We found eHealth monitors user completion rates for the training program on a monthly basis and sends reminders to each respective health sector agency (i.e., Saskatchewan Health Authority, Saskatchewan Cancer Agency, 3sHealth, Ministry of Health) for enforcement. As of June 2022, 89% of users completed information security awareness training.

In addition, we found eHealth established a process in 2021 for its health sector partners to request simulated phishing campaigns at their respective agencies.[5] During 2021, eHealth conducted phishing campaigns at eHealth, 3sHealth, and the Ministry of Health. About 86% of users passed the simulation (e.g., did not click on an attachment or link within the suspicious email). Individuals that did not pass were required to complete an additional training module on cybersecurity and phishing. eHealth expected to conduct its next phishing campaign in November 2022.

Ongoing training reinforces user awareness of good security practices to limit the risk of significant incidents and to protect the eHealth IT network from attacks (e.g., malware).

3.2 Plan to Mitigate Laptop Security Threats and Vulnerabilities in Progress

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

[5] Simulated phishing campaigns are where deceptive emails, similar to malicious emails, are sent by an organization to their own staff to gauge their response to similar phishing and email attacks.

In 2021, eHealth implemented a centralized system to manage and configure laptop devices, updated its standard laptop configuration, and started upgrading laptops to the new standard. However, eHealth needs to complete a formal risk assessment to determine whether they are willing to accept the risks of users' ability to use the USB ports in laptops and their ability to access the device's input/output (i.e., BIOS) settings.[6]

eHealth's IT network houses critical IT health systems and data essential to the delivery of provincial health services. Since 2020, we found eHealth took the following actions to help mitigate security threats and vulnerabilities on laptops with access to the eHealth IT network:

- Implemented a central configuration manager program to manage and configure about 22,000 devices, including laptops, with access to the eHealth IT network.[7,8]

- Updated its standard laptop configuration settings and is working toward upgrading all managed laptops to the new standard. We found the standard configuration aligns with good practice such that it uses a supported operating system (i.e., Windows 10), includes encryption, and does not include CD/DVD burners.[9] We examined three laptops from former health regions that previously used inconsistent system configurations and found all three laptops utilized the new standard configuration settings.

At June 2022, 84% of managed laptops used a supported operating system (i.e., Windows 10). The remaining laptops use Microsoft's Windows 7 Operating System. eHealth plans to implement Windows 10 on its remaining laptops or implement controls to mitigate risks (e.g., network segmentation) by December 2022.

Microsoft no longer supports its Windows 7 Operating System as of January 14, 2020 (i.e., no longer provides security patches or updates). The inability to process security patches and updates does not permit eHealth to provide all of its managed laptops with protection against known vulnerabilities.

Also at June 2022, 71% of devices use encryption. eHealth plans to address encryption issues as it replaces its old laptops in 2023.

Protecting laptops through encryption helps reduce the risk of compromise in the event the laptop is lost or stolen. Encrypted laptops could also protect eHealth from unauthorized individuals gaining access to locally stored passwords and the eHealth IT network.

While eHealth made some improvements to its standard laptop configuration settings, we found eHealth continues to permit unrestricted use of USB ports in laptops. Blocking the

[6] 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. www.techtarget.com/whatis/definition/BIOS-basic-input-output-system (24 August 2022).

[7] Microsoft's System Centre Configuration Manager [SCCM] allows IT staff to manage a large number of Windows-based computers. SCCM features remote control, patch management, operating system (e.g., Windows) deployment, and other various services. SCCM can roll out anti-virus and anti-malware updates, operating system security updates and patches, and security configurations to laptops in a consistent manner.

[8] This includes all eHealth managed laptops and desktops.

[9] Good practice views USBs, CDs, and DVD burners as unsecure tools.

USB ports can prevent devices from downloading data, or uploading malicious software and tools.

In addition, our review of the standard configuration found users have access to the BIOS settings—permitting users to control device settings at the hardware level. eHealth has yet to complete a formal risk assessment to determine whether they are willing to accept the risks of users' ability to use the USB ports in laptops or ability to access the BIOS settings.

3.3 Central Mobile Device Manager Needed

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

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—Partially Implemented

While eHealth made improvements to mobile devices' (e.g., smartphones) auto lock settings and began piloting a central mobile device management tool, it has not fully standardized its configuration settings for mobile devices with access to the eHealth network. Configuration settings continue to not align with good practice in several areas (e.g., password requirements, use of jailbroken or rooted devices, use of containerization).[10,11]

At June 2022, eHealth is responsible for 5,500 mobile devices. eHealth's configuration of mobile devices differs based on each health sector agency (e.g., eHealth, Saskatchewan Health Authority) and location. Since 2019, eHealth uses three mobile device management tools to manage mobile devices with access to the eHealth network. It is piloting one of these systems for implementation as its central mobile device management system for all health sector agencies by the end of 2022–23.

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

[10] Jail Break/Rooting: Bypassing the restrictions placed on the mobile device by the manufacturer. With a jailbroken mobile device, you 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.

[11] 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.

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

- **Auto lock settings aligned with good practice.** We found eHealth configured its mobile device management system to lock mobile devices after five minutes of inactivity—consistent with good practice.

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

  We found eHealth provides guidance to staff on passwords. Its policy requires a password to be at least four characters in length and discourages, but does not prohibit, the use of sequential and repetitive characters. For example, our testing found the standard configuration accepts using '0000' as a password.

  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 these devices may be used to bypass manufacturer restrictions and security protections, exposing the device and eHealth IT network to attack.

  At June 2022, eHealth had yet to complete a formal assessment on mobile device configuration settings and continued to allow jailbroken and rooted devices on the eHealth IT network.

- **Containerization not 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.

  At June 2022, eHealth had yet to complete a formal assessment of containerization. It also continued to not use containerization to segregate corporate and personal applications and data, even though staff can use mobile devices for personal use.

- **No restrictions on application downloads.** Good practice suggests restricting downloads on mobile devices to only corporate-approved applications and stores. Mobile device management systems do not restrict these types of downloads.

  When testing an eHealth-managed mobile device (i.e., smartphone), we found the configuration allowed for unlimited downloading of app store applications. This increases the risk of inappropriate applications downloaded to corporate mobile devices and the risk of users installing malware on corporate mobile devices.

Inconsistent configuration settings on mobile devices results 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.

3.4 Need Coordination with Health Partners to Centrally Track 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—Not Implemented

eHealth does not know the full extent of lost or stolen portable computing devices at the health sector agencies to which it provides services.

While eHealth knows the extent of lost or stolen portable computing devices within its own organization (i.e., zero since our 2020 audit), it does not have a mechanism to centrally track lost or stolen devices it manages for other health sector agencies (e.g., Saskatchewan Health Authority). As a result, eHealth does not know whether it appropriately wiped (i.e., smartphones) or removed from the network (i.e., laptops) all lost or stolen eHealth-managed devices.

Using information obtained from the Saskatchewan Health Authority, we tested a sample of five lost or stolen devices managed by eHealth. For four of the devices tested, we found eHealth was unable to find evidence that the Authority reported the devices to eHealth (i.e., through tickets submitted to its IT service desk), or that it appropriately wiped or removed the devices from the network.

eHealth needs to work with its health sector partners to improve its receipt of notification of all lost or stolen devices so it can appropriately wipe or remove the devices from the network.

Not taking appropriate action to address lost or stolen portable computing devices increases the risk of unauthorized access to the network, putting personal health information at risk.

3.5 Network Access Controls 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 needs to implement its plan to control network access.

eHealth is working toward centralized network access controls for all health sector agencies and network access ports.[12] eHealth plans to pilot network access controls in one medium and one large healthcare facility (e.g., hospital) by the end of March 31, 2023, with full rollout timelines determined after the pilot program.

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

Establishing IT network access controls to restrict the access of users 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.

3.6 Limited Progress on Improved 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 is working to secure a Managed Security Service Provider (MSSP) to help manage the security of the IT network.

eHealth continues to monitor pieces of the eHealth IT network; however, it does not scan all areas of the IT network. eHealth needs additional security tools and monitoring capabilities to detect, prevent and control malicious activity.

At June 2022, eHealth is working to secure a MSSP to manage and monitor security devices and systems. It expects the MSSP will monitor network security on a 24/7 basis and focus on preventing, detecting, analyzing and responding to cybersecurity incidents.

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] 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. www.fortinet.com/resources/cyberglossary/what-is-network-access-control (25 August 2022).