Chapter 6
eHealth—Securing Portable Computing Devices

1.0 Main Points

Portable computing devices (e.g., laptops, smartphones) create security risks for an organization because they are attractive targets for attackers, may become infected with a virus or malware, and are easy to lose.

This chapter reports on the processes eHealth Saskatchewan had to secure health information on portable computing devices from unauthorized access.

At August 2019, eHealth had effective processes, other than in the following areas, to secure health information on portable computing devices. eHealth needs to:

- Adequately configure portable computing devices

  Unsupported and unencrypted laptops make it easier for an attacker to gain access to information stored on the device. Inappropriate security settings on portable computing devices can expose the device, and the eHealth IT network to viruses and malware.

- Regularly train staff on the security threats associated with portable devices

  Uninformed staff are susceptible targets who may click on something that they should not, infecting their device with malware or a virus. This creates a potential access point for malicious software into the eHealth IT network.

- Take appropriate action when devices are reported as lost or stolen

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

- Sufficiently control and monitor the eHealth IT network access to detect and prevent malicious activity

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

Having proper controls over portable computer devices reduces the risk of security breaches including having personal health information fall into the wrong hands.

2.0 Introduction

Portable devices includes smartphones, personal digital assistants, tablets, and laptops. The audit looked at processes for portable devices with the ability to access IT systems for which eHealth is responsible.

2.1 eHealth Saskatchewan—Responsible for Security of Portable Devices

A cabinet-appointed Board oversees eHealth Saskatchewan. The Board is accountable to and reports to the Minister of Health.

eHealth is responsible for managing critical IT services used to administer and deliver health care 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, and 3sHealth.[1,2] The Authority has more than 40,000 employees and over 2,500 physicians.[3]

Since the consolidation of the province's health regions into a single Authority in January 2017, eHealth has been working to consolidate IT services into a single service provided by eHealth.[4]

The December 4, 2017 Operating Agreement for Interim Services with the Authority clearly makes eHealth responsible for managing laptops and mobile devices (e.g., smart phones and tablets) used in the management and delivery of provincial health services. **Figure 1** sets out some of eHealth's specific responsibilities under this agreement. This Agreement remains in effect at January 2020.

Figure 1—eHealth's Responsibilities under December 4, 2017 Operating Agreement for Interim Services

eHealth agrees to provide:

- Computer and Peripheral Setup: eHealth will purchase and supply computers and related equipment. Additionally, eHealth will manage workstations (e.g., laptops) through standard images and updating processes.
- Mobile Device Management: eHealth will purchase, setup, and manage smart phones for authorized staff, and configure mobile devices to access email and calendars.
- Information Security: eHealth will keep devices up-to-date against registered security threats and vulnerabilities (e.g., anti-virus, anti-malware, patching).

As of August 2019, eHealth had about 340 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., vital statistics and provincial health card information).

[1] Saskatchewan Order-in-Council 734-2010.
[2] In addition, eHealth is responsible for administering and operating the *Vital Statistics Act* (2009), the *Change of Name Act* (1985), and the Health Registration Registry. It also has responsibility for procuring, implementing, owning, operating or managing other health information systems.
[3] We refer to these individuals as Authority staff in this report.
[4] www.saskatchewan.ca/government/news-and-media/2017/january/10/transition-to-single-provincial-health-authority-underway (03 February 2020).

2.2 Risks Associated with Use of Portable Computing Devices

Portable devices are attractive targets for attackers. Therefore, effective management of device security is essential. Portable devices present many risks to an organization including, but not limited to:

- Use of portable devices give individuals wireless access to IT systems and data (that is, do not require physically connecting to a corporate IT network). Wireless networks are typically less secure than wired networks.[5] Sending data via a wireless network creates an opportunity for data to be intercepted before it arrives at its intended destination.

- Portable devices' use of public Wi-Fi increases the risk of infecting portable devices with a virus or malware. Without appropriate safeguards, an infected device connecting to a corporate IT network can risk infecting an organization's IT network or portion thereof. Addressing infected IT networks takes time and resources and may affect the availability of IT systems and data.

- Portable device users do not always encrypt documents or data on their devices. Unencrypted information stored on the device is easily obtainable if an attacker gains physical or wireless access to the device (e.g., through theft of the device or through hacking the device).

- The small size of mobile devices make them easier to lose or be taken. Attackers using improperly managed portable devices have a greater likelihood of gaining unauthorized access to the corporate network.

Almost 13,000 (over 30 percent) healthcare providers (including physicians) can access provincial health IT systems through the use of portable devices (e.g., laptops). They use this access to help them manage and deliver health services. These devices can access or may also store private and confidential health information.

Without proper controls over portable computing devices, eHealth risks security breaches including personal health information, falling into the wrong hands. Security breaches may impact eHealth's ability to provide health agencies with access to IT systems and data necessary for effective health service delivery. Unavailable IT systems can in turn affect the ability of the health sector to provide adequate and timely care, and diagnosis to patients.

3.0 AUDIT CONCLUSION

We concluded, for the 12-month period ended August 31, 2019, eHealth Saskatchewan had effective processes, except in the following areas, to secure health information on portable computing devices used in delivery of Saskatchewan health services from unauthorized access.

[5] Mobile devices use wireless networks (e.g., Wi-Fi) to send data between devices.

eHealth needs to enhance and standardize the configuration settings for its portable computing devices. This will mitigate the risk of unauthorized access, breach, or interrupted service through nefarious activities carried out on portable devices.

eHealth also needs to keep staff sufficiently informed of security threats associated with portable devices and take appropriate action when devices are reported as lost or stolen.

Portable computing devices connecting to corporate IT networks creates attack paths for security threats. eHealth needs to sufficiently monitor its network to detect and prevent malicious activity and adequately mitigate impact to its network in the event of an attack.

Figure 2—Audit Objective, Criteria, and Approach

Audit Objective: Assess the effectiveness of eHealth Saskatchewan's processes during the 12-month period ending August 31, 2019 to secure health information on portable computing devices used in the delivery of Saskatchewan health services from unauthorized access.

Audit Criteria: Processes to:

1. Plan to secure portable computing devices against security threats
   - 1.1 Identify risks associated with giving portable computing devices access to systems and data of eHealth and its stakeholders (e.g., Saskatchewan Health Authority, Saskatchewan Cancer Agency)
   - 1.2 Maintain approved policies and related security requirements that address identified risks (e.g., access control rules, data retention, encryption)
   - 1.3 Annually train users of authorized portable computing devices on applicable policies and procedures, and consequences for not adhering to them
2. Enforce policies and procedures
   - 2.1 Grant access only to portable computing devices that are compatible with eHealth's systems and data and required for a business purpose
   - 2.2 Centrally monitor whether authorized portable computing devices comply with eHealth's security requirements (e.g., centrally track, configure, and update devices, remote wipe lost devices) and are used for business purpose
   - 2.3 Apply adequate access control rules
   - 2.4 Maintain up-to-date anti-virus and anti-malware on authorized portable computing devices
   - 2.5 Store and transmit data securely (e.g., backups, encryption)
3. Detect unauthorized portable computing devices
   - 3.1 Routinely review security logs
   - 3.2 Follow effective incident management processes (e.g., help desk, breach response)
   - 3.3 Address identified security threats and policy non-compliance (e.g., revoke access of mobile device) within a reasonable timeframe

Audit Approach: To conduct this audit, we followed the standards for assurance engagements published in the CPA Canada Handbook—Assurance (CSAE 3001). To evaluate eHealth's processes, we used the above criteria based on related work, reviews of literature, and consultations with management. eHealth's management agreed with the above criteria.

Our examination included discussions with eHealth staff, as well as IT staff of the Saskatchewan Health Authority located in Regina and Saskatoon. We examined policies and procedures related to securing and configuring portable computing devices that can connect to the eHealth IT network. We hired an external consultant to assess the configuration of six portable computing devices (i.e., three laptops configured by Regina, Saskatoon, and eHealth and three smartphones deployed from Regina, Saskatoon, and eHealth) against good practice. We also tested a sample of portable computing devices provisioned to eligible users, and a sample of incident reports.

4.0 KEY FINDINGS AND RECOMMENDATIONS

4.1 Security Policies over Portable Computing Devices Generally Reasonable

IT security policies for portable computing devices in use in the provincial health sector generally include sufficient and appropriate high-level direction, even though they vary somewhat in form and content.

At August 2019, eHealth had not yet established a common set of IT security policies for healthcare IT systems which it assumed responsibility for under the January 2017 decision to consolidate IT services into eHealth.[6]

Instead of eHealth mandating the use of its IT security policies for securing portable devices, it allowed agencies with IT staff that had not transitioned into eHealth to continue to use the IT security policies of their agency or former health region. At August 2019, IT staff of the Saskatchewan Health Authority who were part of the former Regina Qu'Appelle and Saskatoon health regions had not yet transitioned to eHealth. In the intervening period, eHealth must continue to identify and mitigate vulnerabilities because of variations in practice.

Figure 3—Breakdown of Number of Portable Computing Devices Accessing the eHealth IT Network by Type and Device Owner as of August 2019

	Laptops		Mobile Devices [A]	
Device Owner	Number of	% of Total	Number of	% of Total
eHealth	227	2.9%	125	2.4%
Ministry of Health, 3sHealth, the Saskatchewan Cancer Agency, and the Saskatchewan Health Authority (other than Regina Qu'Appelle and Saskatoon)	2,816	31.4%	2,408	27.9%
Saskatchewan Health Authority (Former Regina Qu'Appelle health region)	2,394	28.7%	1,472	24.1%
Saskatchewan Health Authority (Former Saskatoon health region)	2,189	37%	1,273	45.6%
	7,626	100%	5.278	100%

Source: Information provided eHealth Saskatchewan.
[A] Mobile devices include smartphones, personal digital assistants, and tablets.
eHealth directly manages the devices noted in the gray-shaded cells.

As shown in **Figure 3**, eHealth directly managed less than one-half of portable devices accessing eHealth's IT network. Also, at least three sets of IT security policies were in use. That is:

- eHealth is using its policies for the portable devices it owns and for those it centrally manages on behalf of others (e.g., former health regions).

[6] The consolidation of IT services into eHealth includes transitioning IT staff of the various health agencies into eHealth.

- The Authority's staff located within the former Regina Qu'Appelle and Saskatoon health regions each use the policies of the former health regions for their portable devices.[7] eHealth expected IT staff to transition into eHealth by January 2020. However, at February 2020, this transition was not yet complete. eHealth noted the transition is taking longer than it anticipated.

Our review of three sets of IT security policies for portable devices found, while variations exist, each had reasonable policies that were generally in line with good practice (e.g., ISO 27002). Each set included direction on user access, storing data, setting passwords, and having anti-virus and anti-malware software.

We also found each set of policies were sufficiently accessible with electronic copies available via the related intranet. In addition, we found the procedures for laptop users to contact the help desk to reset their passwords reasonable.

Consolidating all IT security policies into a single set of overarching policies would reduce complexity and inconsistencies.

We found variations existed in standard configuration settings applied to portable devices (e.g., password requirements, encryption requirements). A few of these variations did not align with good practice. For example, see **Section 4.3** (for laptops) and **Section 4.4** (formobile devices) about making sure portable devices with access to the eHealth IT network are appropriately configured.

4.2 More Frequent User Awareness Training Needed for Users of Portable Computing Devices

eHealth has not set minimum confidentiality and privacy training requirements for individuals accessing the eHealth IT network through use of portable computing devices.

As shown in **Figure 3**, the staff of the Saskatchewan Health Authority account for the majority of individuals accessing the eHealth IT network through use of portable devices.

eHealth and the Authority each have their own user awareness security training programs. At August 2019, the Authority had staff in about 40,000 full-time equivalent positions (FTEs); eHealth had about 340 FTEs.

We found the content of each training program sufficient for users accessing the eHealth IT network through use of portable devices. For example, both training programs include information on protecting personal health information (e.g., protecting portable devices from theft, loss, or unauthorized disclosure of information), and acceptable use of portable devices (e.g., do not access websites with known malicious software such as pornographic or illegal video streaming sites).

In addition, both eHealth and the Authority require staff to complete a test on the training received to show their awareness.

[7] Saskatchewan Health Authority continues to own portable computing devices and had voluntarily adopted the same anti-virus/ anti-malware technology as eHealth.

However, the frequency of the training differs. We found:

- Consistent with good practice, eHealth requires its staff to complete confidentiality and privacy training each year.[8] In addition, eHealth requires staff to annually acknowledge their compliance with eHealth's code of conduct including acceptable use of IT assets.

- The Authority is aiming to have staff complete training every three years. The Authority's goal is to have 21,900 staff (of its over 40,000 staff) complete the training by March 31, 2020, and all staff complete the training by March 31, 2021. The Authority requires staff to sign a standard Confidentiality Agreement upon being hired; it refers to its security policies and procedures.

eHealth has not asked the Authority to place priority on training Authority staff using portable devices accessing the eHealth IT network.

As of December 2019, we found all eHealth staff completed the training for the 2019-20 fiscal year, and about 21,400 Authority staff completed the training. As **Figure 4** explains 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).

Figure 4—Importance of IT Security Awareness Training

Training reinforces that hackers are particularly interested in sensitive and confidential information (like health data). It helps staff know, while having an anti-virus program is an important first step, anti-virus programs cannot always protect from a user's computer behaviors like clicking on harmful links or failing to update software. Informed staff are less likely to open email attachments containing malware, or download applications that can infect a device which in turn may impact a corporate IT network.

Source: Brodie, Cindy. (2008). The Importance of Security Awareness Training. (www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013). (04 February 2020).

The importance of awareness training is higher for staff using portable devices because those devices can pose security risks beyond those of wired computers. Awareness training informs device users of security threats and vulnerabilities associated with their devices. Informed staff are more likely to keep the operating systems of devices up-to-date, limit the data kept on their devices, use a strong password, and report lost/misplaced devices immediately.

Furthermore, IT security threats and vulnerabilities can change quickly with confidential and private information (like health information) increasingly the target of attacks. These factors increase the importance of providing training sufficiently frequently to keep device users informed about the latest malware.

1. **We recommend 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.**

[8] www.isaca.org/resources/isaca-journal/past-issues/2011/jonline-impact-of-security-awareness-training-components-on-perceived-security-effectiveness (04 February 2020).

4.3 Robust Plan to Mitigate Laptops Security Threats and Vulnerabilities Needed

eHealth's plan to manage health sector laptops is not sufficiently robust. It does not contain sufficient detail on how to mitigate security threats and the vulnerabilities of laptops with access to the eHealth IT network. This network houses critical IT health systems and data essential to the provincial delivery of health services.

Since December 2017 (through the Operating Agreement for Interim Services with the Saskatchewan Health Authority), eHealth has been responsible for keeping Authority laptops up-to-date against security threats and vulnerabilities. Yet, at August 2019, eHealth directly managed only about one-third of laptops with access to the eHealth IT network (about 3,000 laptops). The Authority managed the rest.

Anti-virus and anti-malware software used: eHealth is actively managing the use of anti-virus and anti-malware software. Good practice suggests the use of such software as one of many lines-of-defence to safeguard against security threats.

We found eHealth gave Authority IT staff direction about approved versions of anti-virus and anti-malware to deploy onto laptops, and when to apply laptop operating system security updates. We found anti-virus, anti-malware, and patches applied to both eHealth and Authority laptops was up-to-date.

Central management plan contingent on timing of transition of all IT staff: As of August 2019, eHealth has documented plans to centrally manage all laptops with access to the eHealth IT network. Plans include expanding its current use of a central configuration manager program (i.e., Microsoft's System Centre Configuration Manager [SCCM]) once the transition of IT staff from the Authority into eHealth is complete. As **Figure 5** describes using configuration manager programs, like SCCM, can help manage and configure large number of laptops efficiently and consistently.

Figure 5—Brief Description of Microsoft's System Centre Configuration Manager (SCCM)

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.

Source: www.computerhope.com/jargon/s/sccm.htm. (04 February 2020).

Provisioning processes followed: At August 2019, at least three sets of laptop provisioning processes, and standard configuration settings were in place (e.g., eHealth, Saskatchewan Health Authority—former Regina Qu'Appelle health region [Regina], and Saskatchewan Health Authority—former Saskatoon health region [Saskatoon]).

Our testing of 30 laptops provisioned during the 12-month period ending August 2019 found supervisors properly approved providing staff with corporate laptops, consistent with the relevant provisioning process.

Configuration settings vary: At August 2019, our review of each set of standard laptop configuration settings, and test of three laptop configurations found the configuration and

operating systems on eHealth-managed, Regina–managed, and Saskatoon-managed laptops varied.

We also found eHealth did not have sufficient plans to mitigate security threats and vulnerabilities associated with these variations in configurations and operating systems—in particular security threats and vulnerabilities associated with the following:

- Unencrypted laptops
- Laptops using unsupported operating systems
- Unrestricted USB ports or CD/DVD burners on laptops

Risks associated with unencrypted laptops not mitigated: We found over 80 percent of the laptops with access to the eHealth IT network are not encrypted. When eHealth configures a laptop, it encrypts the laptop; whereas Regina and Saskatoon do not.

As of January 2020, eHealth does not have plans to encrypt all laptops with access to the eHealth IT network.

Our testing of the strength of laptop configuration for each organization found two laptops were not set up in a way to stop unauthorized access to data stored on the laptop, primarily because of the lack of encryption.

From September 2018 to August 2019, eHealth staff and the Authority staff in Regina and Saskatoon reported 49 incidents of stolen or lost laptops. We noted one instance where an unencrypted laptop was stolen that contained personal health information.[9]

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

Risks associated with unsupported operating systems not mitigated: eHealth is aware that over 80 percent of laptops with access to the eHealth IT network use Microsoft's Windows 7 Operating System (an unsupported operating system as of January 2020). Staff of the Authority use most of these laptops.

As of January 2020, eHealth had not determined when or how much it would cost to upgrade the operating systems of these laptops and/or replace the laptops. In addition, it had not determined who is responsible for the related costs.

Microsoft no longer supports its Windows 7 Operating System as of January 14, 2020 (i.e., no longer provides security patches or updates). Security patches and updates provide protection against known vulnerabilities.

Laptops using operating systems that exceed their end-of-support dates are susceptible to compromise and failure. Without regular security patches and updates, these laptops are vulnerable to unauthorized access, resulting in an increased risk of malware and

[9] This incident was reported to the Office of the Saskatchewan Information and Privacy Commissioner.

ransomware attacks successfully breaching data (like personal health information). In addition, not keeping laptops sufficiently secure can place IT systems on the eHealth IT network at risk.

Risks associated with use of USB ports and CD/DVD burners not mitigated: in August 2019, we found laptops in use by the Authority staff in Regina and Saskatoon with CD and DVD burners installed and operating. Good practice views USBs, CDs, and DVD burners as insecure tools.

eHealth did not have plans to limit the use of USBs, CDs, or DVD burners in laptops. Rather it permits the use of any USB device on laptops with access to the eHealth IT network. It allows the purchase of laptops with CD/DVD burners installed, and does not require restricting access to only staff with documented business needs.

We recognize situations may exist where staff have a business need for using these unsecured tools. For example, certain units in the hospitals may require access to DVD burners where clinical applications are only compatible with provided data on a DVD. Good practice treats such situations as exceptions, and only grants access to these unsecure tools after identifying and documenting business need, and taking appropriate mitigation steps (e.g., training and supervision).

Blocking the USB ports can prevent devices from downloading data, or uploading malicious software and tools. USBs, CD's and DVD's can store large amounts of data. Disabling use of USB ports or CD/DVD burners can prevent a means to copy confidential data from the laptop. Appropriately restricting users from transferring data via portable devices can control sensitive and confidential health information from leaving the care and control of eHealth.

2. **We recommend eHealth Saskatchewan implement a written risk-informed plan to protect laptops with access to the eHealth IT network from security threats and vulnerabilities.**

Because eHealth is managing IT systems and data on behalf of various health agencies, it must also ensure a clear understanding exists over the responsibilities of each party for these activities including who is responsible for the costs of them. As shown in **Figure 3**, staff of the Authority use most of the laptops with access to the eHealth IT network. See **Chapter 3** of our *2019 Report —Volume 2* (p. 29) about eHealth's need for an adequate service level agreement with the Authority. At January 2020, such an agreement was not yet in place.

4.4 Central Management of Mobile Devices Needed

eHealth does not have a plan to properly secure corporate-owned mobile devices (e.g., smart phones, and tablets) with access to the eHealth IT network.[10] As previously noted, this network houses critical IT health systems and data essential to the management and delivery of provincial health services.

[10] Each organization with access to the eHealth IT network (i.e., eHealth, Saskatchewan Health Authority, 3sHealth, Saskatchewan Cancer Agency, and the Ministry of Health) owns their own corporate mobile devices.

Since December 2017, eHealth is responsible for about 5,000 mobile devices. As of August 2019, it only directly manages about 125 mobile devices. Other health sector agencies (e.g., Saskatchewan Health Authority) own and manage the rest. Corporate-owned mobile devices have access to email, contacts, and calendars only.

At least three sets of mobile device provisioning processes, and standard configuration settings were in place (e.g., eHealth, Saskatchewan Health Authority—former Regina Qu'Appelle health region [Regina], and Saskatchewan Health Authority—former Saskatoon health region [Saskatoon]). We tested three sets of mobile device provisioning processes, and standard configuration settings.

Provisioning processes followed: Our review found each set requires a supervisor approval before staff receive a mobile device. eHealth manages the mobile devices it owns, and the Authority manages the mobile devices that it owns. Each respective party pays for the mobile devices it owns.

Our testing of 30 mobile devices granted during the 12-month period ending August 2019 found supervisors properly approved providing corporate mobile devices to staff, consistent with the relevant provisioning processes.

Configurations vary: Our review of each mobile device configuration settings, and testing of each mobile device configurations found both similarities and variations.

We found the following similarities:

- Each used a standard configuration setting to set up their corporate mobile devices, and how they accessed the eHealth IT network.
- Each enabled GPS tracking on corporate mobile devices.
- Each can wipe a device in the cases where the corporate mobile device is lost or stolen (wiping a device makes data stored on the device unreadable and inaccessible).
- Each expected users of corporate mobile devices to accept and apply patches and updates to their device's operating systems as issued by vendors (e.g., Apple, Samsung).
- Both eHealth and Regina used a mobile device management system (albeit different ones) to help manage their corporate mobile devices; Saskatoon did not.

We also identified the following differences in the configuration of corporate mobile devices; some of which do not align with good practice:

- **Not all jailbroken/rooted devices blocked**:[11] Consistent with good practice, two of the three configurations were set to block devices that have been jailbroken or rooted; this was done through the use of a mobile device management system. One mobile device configuration did not have the capability to block this activity, as a mobile device management system was not used.

[11] Jail Break / Rooting: Bypassing the restrictions placed on the mobile device by the manufacturer. With a jailbroken mobile device, you can install apps and setting changes not authorized by the manufacturer. Additionally, you remove the default security protections built into the mobile device by the manufacturer.

A jailbroken mobile device allows users to bypass manufacturer restrictions and security protections on their smartphones, thereby exposing the devices, and the eHealth IT network to viruses and malware.

At January 2020, eHealth did not have a documented plan to move towards a central mobile device management system.

- **Password settings do not align with good practice**: Two of the three standard configuration settings require a minimum password Personal Identification Number (PIN) of four characters. Good practice recommends six characters.

  At August 2019, eHealth had not set minimum password requirements for all corporate mobile devices with ability to access the eHealth IT network.

- **Unlimited downloading of applications allowed**: All three of the standard configuration settings did not limit the number of or types of applications users can download onto corporate mobile devices. None restricts applications to those with a business purpose (e.g., no social media, no games) or requires users to seek approval before downloading applications.

  Good practice recommends restricting which applications may be installed and from where.[12] Allowing downloading of unapproved applications increase the risk of users installing malware on corporate mobile devices. Devices infected with malware can pose a security risk to the organization, its corporate network, and data.

  At August 2019, eHealth did not have plans to place limits on applications users can download.

- **Auto Lock setting too lengthy**: One of the three standard auto-lock settings is set to one hour instead of a shorter timeframe; good practice suggests a short-period of time (e.g., five minutes).[13]

  Auto-lock automatically closes the display on a mobile device when it remains idle. Automatically closing the display minimizes risk of snooping, and requires a user to re-enter the devices password to unlock the device. With a long auto-lock period, a user may leave their mobile device unattended and unlocked, increasing the risk of loss of sensitive data.

  At August 2019, eHealth did not have plans to enforce a consistent auto lock setting for all mobile device users.

- **Containerization Not Used**:[14] Neither eHealth nor the Authority use containerization to separate users' personal usage from their corporate usage even though both allow staff to use corporate mobile devices as their personal devices.

[12] nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. (05 February 2020).
[13] nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. (05 February 2020).
[14] 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.

Co-mingling personal and corporate use on a device increases the risk of sharing sensitive data publicly, either intentionally or unintentionally. Best practice suggests use of containerization of corporate mobile devices to help secure corporate confidential data.

At August 2019, eHealth did not have plans to consider containerization.

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. Additionally, without appropriate password settings or security settings (e.g., auto-lock settings) lost or stolen mobile devices are a potential access point for malicious software into the eHealth IT network.

3. **We recommend eHealth Saskatchewan standardize the configuration settings for mobile devices with access to the eHealth IT network to mitigate associated security threats and vulnerabilities.**

Organizations can efficiently enforce consistent configuration of mobile devices through use of a central mobile device management system. Such a system provides corporate data segregation, email security, enforcement of configuration settings (e.g., password settings), device tracking (e.g., in instances of a lost or stolen device), and device usage. Additionally, it can be used to lock and wipe the hard drive of a device.

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

4. **We recommend 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.**

4.5 Management of Personal Mobile Devices with Access to Corporate Information Needed

eHealth does not manage personal mobile devices with ability to access corporate email, contacts, and calendars only.

Neither eHealth nor the Saskatchewan Health Authority (Saskatoon) monitor whether users complete a registration with them before downloading ActiveSync on their personal device.[15] Even though, both require users who wish to register their personal devices on ActiveSync to complete an exemption form beforehand. ActiveSync gives users access to their corporate email.

We found eHealth does not know the number of and types of unmanaged personal mobile devices that remotely access corporate email via the eHealth IT network. We found 56 users at eHealth with ActiveSync downloaded on their personal devices who had not completed an exception form.

[15] ActiveSync is a mobile data synchronization application developed by Microsoft. It synchronizes data with handheld devices and computers (desktop computers, or laptops).

Unmanaged mobile devices are not subject to minimum security settings (e.g., GPS tracking, wiping capability, passwords) in use for managed mobile devices. At times, corporate emails may contain private and confidential health information. If lost or stolen, unmanaged mobile devices present a risk of exposing confidential information. See **Recommendations 3** and **4** about having standardized configuration settings and central corporate management of all mobile devices with access to the eHealth IT network.

4.6 Lost and Stolen Portable Devices Not Always Acted On

Although adequate processes exist to appropriately minimize security risks associated with lost or stolen laptops and mobile devices, they are not always followed.

Consistent with its IT security policies, at August 2019, at least three sets of incident management policies were in place (e.g., eHealth, Saskatchewan Health Authority—former Regina Qu'Appelle health region, and Saskatchewan Health Authority—former Saskatoon health region).

Our review of three sets of incident management policies found they allowed for a quick and effective response to incidents including those involving portable devices with access to the eHealth IT network. In general, they require staff to promptly report details about the incident to a relevant IT department, and the IT department to address the incident and to document the actions taken. For example,

- For reported lost or potentially stolen laptops, IT staff are to remove the laptop from the eHealth IT network to prevent access to the network.

- For reported lost or potentially stolen mobile devices, IT staff are to cancel the mobile plan and wipe the device. Wiping a device makes data stored on the device unreadable and inaccessible.

For the twelve-month period ending August 2019, staff reported 14 incidents of lost or potentially stolen portable devices.

In three of 14 such incidents, IT staff did not take action consistent with the IT incident management policies. That is, the laptop's access to the eHealth IT network was not removed, or a lost mobile device was not wiped. For one other incident, IT staff did not keep evidence of action taken.

Not properly wiping the lost or stolen mobile device, or removing the lost or stolen laptop from the eHealth IT network increases the risk of unauthorized access to the network and private and confidential health information.

5. **We recommend eHealth Saskatchewan take appropriate action to minimize the risk of security breaches when a portable computing device is reported lost or stolen.**

4.7 Evaluation of IT Network Access Controls Needed

eHealth does not sufficiently control access to the eHealth IT network, nor has it evaluated the effectiveness of its network access controls.

eHealth does not restrict where users and devices can go on the eHealth IT network and what they can do.

Our testing of the security configuration of two of three laptops was able to bypass laptop security (e.g., compromise local administrative credentials) and gain access to the eHealth IT network. Therefore, the standard configuration settings used for the two laptops tested did not provide an effective level of protection from unauthorized access (see **Recommendation 2**).

To protect against the many ways an attacker may attempt to gain access to systems and data, good practices suggest the use of a defence-in-depth strategy. The principle of defence-in-depth is that layered security mechanisms increase security of the IT system as a whole. If an attacker causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system. For example, establishing IT network access control restricts the access of users to only what they need, making 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.

The connection of portable devices to corporate networks creates attack paths for security threats. The more portable devices that connect, the greater the risk of the corporate network being breached. Controlling IT network access helps mitigate the risk of security breaches, and the extent of breaches.

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

4.8 Monitoring of Unauthorized Network Access Limited

eHealth is not effectively monitoring network security logs to detect and prevent malicious activity on the eHealth IT network.

At August 2019, eHealth's IT Security team (including the Chief Security Officer) consisted of staff in 3.5 full-time equivalent positions. This team is responsible for monitoring the eHealth IT network.

We found that eHealth performs limited monitoring of its IT network to identify if unauthorized individuals have access, or actively search the network for sensitive information (e.g., passwords, personal health information). At August 2019, eHealth was not using network security equipment to log security alerts, errors, and warning messages to detect malicious activity on the network, such as reports related to vulnerability scans, network usage, potential security violations like invalid login attempts, or unauthorized attempts to modify sensitive servers or files.

In addition, since 2018, eHealth did not produce and monitor reports about patch management activities.

As noted in **Section 2.2**, portable devices can present additional security risks if not properly configured or monitored. As noted in **Sections 4.3** and **4.4**, eHealth needs to do more to better secure laptops and mobile devices with access to the eHealth IT network.

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.

7. **We recommend eHealth Saskatchewan utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity.**

5.0 GLOSSARY

Application – A software program. This includes programs such as word processors, spreadsheets, database programs, accounting programs, etc.

Configuration – To set up or arrange in order to achieve a specific purpose (e.g., maximize security)

Encryption – The process of converting information or data into a code, especially to prevent unauthorized access.

Malware – Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Malicious Activity – External or internal threats to a corporate network and could potentially have impact on the confidentiality, integrity, and availability of data.

Network – A group of computers that communicate with each other

Patch – An update to a computer program or system designed to fix a known problem or vulnerability.

Ransomware – Malicious software designed to block access to a computer system and its files until a sum of money is paid.

Server – A computer that hosts systems or data for use by other computes on a network.

Unauthorized access – When someone gains access to a website, program, server, or other systems and data using someone else's account or other methods.

6.0 SELECTED REFERENCES

Auditor General of British Columbia. (2016). *Management of Mobile Devices: Assessing the Moving Target in B.C.* Victoria: Author.

Auditor General of Manitoba. (2015). *WRHA's Management of Risks Associated with End-user Devices.* Winnipeg: Author.

Cook, I. (2017). *ISACA Journal, Volume 6*, 2017, *IS Audit Basics: Auditing Mobile Devices*. www.isaca.org/resources/isaca-journal/issues/2017/volume-6/is-audit-basics-auditing-mobile-devices. (December 17, 2019).

Information Systems Audit and Control Association. (2010). *An ISACA Emerging Technology White Paper, Securing Mobile Devices*. Illinois: Author.

Information Systems Audit and Control Association. (2010). *Mobile Computing Security Audit/Assurance Program*. Illinois: Author.

Information Systems Audit and Control Association. (2010). *Bring Your Own Device (BYOD) Security Audit/Assurance Program*. Illinois: Author.

National Institute of Standard and Technology. (2013). *NIST Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Maryland: Author.

Provincial Auditor Saskatchewan. (2016). *2016 Report – Volume 1, Chapter 6, Central Services – Web Application Security Requirements*. Regina: Author.