Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 009-2020, 053-2020, 224-2020

eHealth Saskatchewan
Saskatchewan Health Authority
Ministry of Health

January 5, 2021

Summary: eHealth Saskatchewan (eHealth), the Saskatchewan Health Authority (SHA) and the Ministry of Health (Health) were the victims of a ransomware attack in late December 2019 and early January 2020, resulting in approximately 40 gigabytes of encrypted data being stolen from eHealth by malicious actors. As a result of the investigation, the Commissioner made several findings and recommendations. Some of these include the Commissioner found there was a privacy breach containing personal information and personal health information of individuals. The Commissioner found that eHealth failed in fully investigating the two early threat occurrences, which may have prevented the malicious extraction of data that followed. The Commissioner found that eHealth, the SHA and Health failed to contain the breach. The Commissioner found that eHealth did not sufficiently provide notification and that the SHA and Health failed in their notification efforts due to the excessive delay in providing notification. The Commissioner found that the SHA did not provide the employee at the heart of the incident with training on its Acceptable Use of IT [Information Technology] Assets policy. The Commissioner also found that eHealth failed its duty to protect the personal information and the personal health information of the citizens of Saskatchewan as a government institution, a trustee and an Information Management Service Provider (IMSP) for Health, the SHA and eHealth's partners. The Commissioner also found that the SHA and Health failed their duty to protect that same information without having all the necessary checks and balances in place to ensure that eHealth, their IMSP, was not handling their IT service delivery in a deficient manner. The Commissioner found that although eHealth, the SHA and Health provided his office with some preventative measures, they were not comprehensive or detailed. The Commissioner recommended that eHealth utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity. The Commissioner also recommended that eHealth

undertake a comprehensive review of its security protocols to include an in-depth investigation when early signs of suspicious activity are detected. The Commissioner recommended that eHealth continue dark web monitoring for a minimum of five years from the date of this Report. The Commissioner further recommended the SHA and Health take immediate steps to provide mass notification including media releases, newspaper notices, website notices and social media alerts. The Commissioner recommended eHealth, the SHA and Health work together and provide identity theft protection, including credit monitoring, to affected individuals for a minimum of five years from the date an affected individual's information is discovered on the dark web or to any concerned citizen who requests it. In addition, the Commissioner recommended eHealth review and reconsider the 70% cyber security training pass mark for its employees and its partners' employees and increase the pass mark to a minimum of 90%. The Commissioner recommended that eHealth review whether it should have IT security staff in place 24 hours a day, seven days a week to actively monitor and investigate potential threats. Finally, the Commissioner recommended that the Minister of Health immediately commence an independent governance, management and program review of eHealth based upon the concerns put forward by Saskatchewan Telecommunications, the Provincial Auditor and this Report.

I BACKGROUND

[1] On January 10, 2020, eHealth Saskatchewan (eHealth) reported a cyberattack on its computer systems and confirmed publicly that it was subject to a ransomware attack.

[2] On January 16, 2020, my office issued a media release advising that we would be investigating whether there was a breach of personal information [pursuant to *The Freedom of Information and Protection of Privacy Act* (FOIP)] or personal health information [pursuant to *The Health Information Protection Act* (HIPA)] and if so, the circumstances leading to it and what measures eHealth could have taken to prevent it. The news release also advised that my office would also be investigating ways eHealth can help ensure the future security of this information and avoid further attacks.

[3] Once my office had completed some cursory background work, on January 29, 2020, my office notified eHealth that it would be undertaking a privacy breach investigation into this

matter and requested a copy of eHealth's investigation report and other supporting documentation.

[4] My office met with eHealth on February 27, 2020, for an update on its investigation efforts. During that meeting, my office was advised that the ransomware entered the eHealth computer systems and networks through the actions of a Saskatchewan Health Authority (SHA) employee.

[5] On March 4, 2020, my office notified the SHA that it would be undertaking a privacy breach investigation pursuant to subsection 52(d) of HIPA. My office requested a copy of the SHA's investigation report and supporting documentation.

[6] Although my office had been receiving updates from time-to-time from eHealth and the SHA, my office had not received the privacy investigation reports from either organization by late spring 2020. On June 16, 2020, my office introduced the *Privacy Breach Questionnaire for Public Bodies* (Questionnaire) to assist public bodies and trustees in providing our office with the details it requires to complete an investigation. On May 19, 2020, my office provided the SHA with a Questionnaire that it could complete and submit to my office in lieu of an investigation report. My office forwarded the same to eHealth on July 9, 2020.

[7] Although the investigation efforts were occurring throughout the COVID-19 pandemic, my office experienced excessive delays in receiving the completed investigation reports and the Questionnaires from eHealth and the SHA. Therefore, my office emailed eHealth and the SHA on August 28, 2020, and advised that the final due date to submit the completed Questionnaires and supporting documentation was September 30, 2020. Further, if they were not received by that date, my office would proceed to drafting its report on October 1, 2020. Both eHealth and the SHA met the final deadline.

[8] On September 15, 2020, over eight months after the initial ransomware attack was discovered by eHealth, the Ministry of Health (Health) contacted my office. In that telephone discussion, my office was advised that Health recently learned from eHealth that

it was also a victim of the eHealth ransomware attack. Health forwarded me a copy of an eHealth letter it received August 14, 2020 (one month earlier) advising that Health's network may also have been compromised. The letter referenced an 870 page technical report prepared by Saskatchewan Telecommunications (SaskTel) dated May 4, 2020.

[9] On September 16, 2020, my office notified Health that it would be undertaking an investigation into the matter pursuant to section 33 of FOIP and section 52 of HIPA. My office requested Health provide my office with a completed Questionnaire and the 870-page technical report dated May 4, 2020. The due date for the completed Questionnaire and 870-page technical report was October 15, 2020. Health requested a short extension and provided it's completed Questionnaire to my office on October 29, 2020. eHealth forwarded my office a copy of the technical report.

II DISCUSSION OF THE ISSUES

1. Is FOIP, HIPA or *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) engaged and do I have jurisdiction in this matter?

[10] eHealth is a "government institution" pursuant to subsection 2(1)(d)(ii) of FOIP. Health is a "government institution" pursuant to subsection 2(1)(d)(i) of FOIP. The SHA is a "local authority" pursuant to subsection 2(f)(xiii) of LA FOIP.

[11] eHealth and Health each qualify as a "trustee" pursuant to subsection 2(t)(i) of HIPA and the SHA is a "trustee" pursuant to subsection 2(t)(ii) of HIPA.

[12] I will go further into the details of this incident later in this Report. However, this incident occurred because an SHA employee opened an infected Microsoft Word document on two occasions which deployed the ransomware and infiltrated eHealth, SHA and Health computer networks. This infiltration ultimately led to files being extracted from the networks by the malicious actors.

[13] In order for FOIP and LA FOIP to be engaged, there must be "personal information" involved as defined in subsections 24(1) of FOIP and 23(1) of LA FOIP. In order for HIPA to be engaged, there must be "personal health information" involved as defined in subsection 2(m) of HIPA.

[14] eHealth advised my office of the following in its completed Questionnaire:

> - The affected servers contain approximately 50 [million] files across eHealth, the Ministry of Health, and the SHA. eHealth performed a metadata scan on the files to determine which files may contain [personal information] and/or [personal health information]. The metadata scan identified approximately 5.5 [million] files [that may contain personal information and/or personal health information].
> …
> - eHealth's Information and Analytics Services team developed a tool that takes parameters that may indicate the presence of [personal information and/or personal health information] (e.g., a nine-digit number that may indicate the presence of a health services number) and is able to scan the files and identify files containing those parameters. A sample of 1,000 files was given to each of eHealth, the Ministry, and the SHA to manually review to test the accuracy of the tool and to make adjustments. The tool was then used to scan the 5.5 [million] files.
> …

[15] eHealth advised my office that of the 5.5 million files identified in the initial metadata scan as potentially containing personal information and/or personal health information, once the above-noted tool developed by eHealth scanned the 5.5 million files, a total of 547,145 files were identified as potentially containing personal information and/or personal health information between eHealth, Health and the SHA.

[16] As noted above, only 3000 of the 5.5 million files were manually checked by eHealth, Health and the SHA to determine the accuracy of the tool. Therefore, I am not able to comment on how accurate the tool is. Further, I am unable to conclude how many files containing personal information and/or personal health information were potentially infected by the malware and potentially extracted from eHealth, Health and the SHA by the malicious actors.

[17] The definition of "personal information" can be found in subsection 24(1) of FOIP and subsection 23(1) of LA FOIP. Subsection 24(1) of FOIP provides:

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form….

[18] Subsection 23(1) of LA FOIP shares substantially similar language.

[19] Subsections 24(1)(a) to (k) of FOIP and subsections 23(1)(a) to (k) of LA FOIP provide examples of types of information that could be considered personal information under FOIP and LAFOIP; however it is not an exhaustive list of examples. In order to qualify as personal information under FOIP and LA FOIP, the following two criteria must be met:

1. Is the information about an identifiable individual?
2. Is the information personal in nature?

[20] The definition of "personal health information" can be found in subsection 2(m) of HIPA, which provides:

> **2** In this Act:
>
> (m) **"personal health information"** means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or
>
> (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;

[21] Based on the information provided to my office, the data that was exposed to the ransomware contains both personal information pursuant to FOIP and LA FOIP and personal health information pursuant to HIPA.

[22] Therefore, I find that there are government institutions, a local authority and trustees involved along with personal information and personal health information of individuals. Therefore, FOIP, LA FOIP and HIPA are engaged and I have jurisdiction to investigate this matter.

2. Did eHealth, the SHA and Health respond appropriately to the privacy breach?

[23] I would like to first express that this is one of the largest privacy breaches that has occurred in this province. However, because the data that was extracted was encrypted, eHealth, the SHA or Health will never know what personal information or personal health information of the citizens of Saskatchewan has been stolen by the malicious actors.

[24] Before I determine if eHealth, the SHA and Health responded appropriately to this breach I will outline the relationship between each of them and provide a chronology of what occurred.

[25] eHealth is a treasury board crown. Page 9 of the *2019-20 Annual Report* for eHealth (available at www.ehealthsask.ca), outlines the key roles of eHealth from its mandate. This includes:

- Consolidate all the Information Technology (IT) Services that were provided by former Saskatchewan health regions, Saskatchewan Cancer Agency (SCA) and 3sHealth into a single service provided by eHealth.
- Lead Saskatchewan Electronic Health (EHR) planning ad strategy for the Province of Saskatchewan.
- Administer and operate the Health Registration Registry.
- Procure, implement, own, operate or manage other health information systems.

- Enter into agreements or arrangements to market IT or expertise to other governments, international agencies, or commercial or non-profit organizations.

[26] eHealth is an information management service provider (IMSP) for the SHA and Health, as well as other health organizations. FOIP, LA FOIP and HIPA include provisions for IMSPs. Subsections 2(1)(e.1) of FOIP and 2(e.1) of LA FOIP define IMSPs, and both subsections share substantially similar language. Subsection 2(1)(e.1) of FOIP provides:

> **2**(1) In this Act:
>
> …
> (e.1) **"information management service provider"** means a person or body that:
>
> (i) processes, stores, archives or destroys records of a government institution containing personal information; or
>
> (ii) provides information or information technology services to a government institution with respect to records of the government institution containing personal information;

[27] Sections 24.2 of FOIP and 23.2 of LA FOIP share substantially similar language and outline the requirements and responsibilities placed on provincial government institutions and local authorities when entering into a relationship with an IMSP. Subsection 24.2 of FOIP provides:

> **24.2**(1) A government institution may provide personal information to an information management service provider for the purposes of:
>
> (a) having the information management service provider process, store, archive or destroy the personal information for the government institution;
>
> (b) enabling the information management service provider to provide the government institution with information management or information technology services;
>
> (c) having the information management service provider take possession or control of the personal information;
>
> (d) combining records containing personal information; or
>
> (e) providing consulting services.

> (2) Before disclosing personal information to an information management service provider, a government institution shall enter into a written agreement with the information management service provider that:
>
> (a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the personal information;
>
> (b) provides for the protection of the personal information; and
>
> (c) meets the requirements of this Act and the regulations.
>
> (3) An information management service provider shall not obtain access to, use, disclose, process, store, archive, modify or destroy personal information received from a government institution except for the purposes set out in subsection (1).
>
> (4) An information management service provider shall comply with the terms and conditions of the agreement entered into pursuant to subsection (2).

[28] In HIPA, an IMSP is defined in subsection 2(j), which provides:

> **2** In this Act:
>
> …
> (j) **"information management service provider"** means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information and includes a trustee that carries out any of these activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf;

[29] Further, section 18 of HIPA outlines the requirements and responsibilities placed on trustees when entering into a relationship with an IMSP:

> **18**(1) A trustee may provide personal health information to an information management service provider:
>
> (a) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee;
>
> (b) to enable the information management service provider to provide the trustee with information management or information technology services;

> (c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; or
>
> (d) for the purpose of combining records containing personal health information.
>
> (2) **Not yet proclaimed.**
>
> (3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).
>
> (4) **Not yet proclaimed.**
>
> (5) If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

[30] In short, eHealth has entered into IMSP agreements with the SHA and Health to deliver IT and IT support services on behalf of the SHA and Health. Both the SHA and Health provided my office with its current service delivery agreements.

[31] The SHA provided my office with a copy of the interim agreement between the SHA and eHealth. The interim agreement was sent to the SHA by eHealth's Interim CEO on April 1, 2018, and was accepted and agreed to on June 5, 2018, by the Chief Executive Officer (CEO) of the SHA. The SHA and eHealth continue their relationship under the terms of the interim agreement.

[32] The interim agreement includes an interim period plan, which is the "…detailed interim period plan to be jointly developed by the parties to detail how the IT Services will be provided by eHealth to the SHA during the Interim Period…." The interim period plan includes several steps including the development of an IMSP agreement, development of a risk assessment and mitigation plan and a technology and security plan.

[33] Health has an IMSP agreement in place with eHealth. It was signed in April 2011, and the agreement's terms are indefinite. I will be discussing the IMSP Agreements in further detail later in this Report.

[34] I find eHealth is an IMSP for the SHA and Health pursuant to FOIP, LA FOIP and HIPA.

[35] In addition to being an IMSP, eHealth is also a government institution under FOIP and a trustee under HIPA. For example, eHealth administers and operates *The Change of Name Act, The Vital Statistics Act,* the provincial Health Registration Registry and the provincial Electronic Health Registry. As such, eHealth has possession and control of personal information pursuant to FOIP and custody and control of personal health information pursuant to HIPA.

[36] The following summary is a high level overview of what occurred. On December 20, 2019, an SHA employee opened an infected Microsoft Word document from their personal email account on their personal device while the personal device was charging by a USB chord on their SHA workstation.

[37] The infected Microsoft Word document triggered the execution of ransomware on the workstation and a multi-phase exploit took place between December 20, 2019 and January 5, 2020. This ultimately led to a Ryuk ransomware (Ryuk/ransomware) attack on January 5, 2020, where the attackers made a ransomware demand. Ryuk is, "…a type of crypto-ransomware that uses encryption to block access to a system, device, or file until a ransom is paid…" (http://cissecurity.org/, accessed October 30, 2020). This is when eHealth first learned of the attack – 17 days after the ransomware infiltrated the network. The attack affected fileshares with eHealth, the SHA and Health due to the shared infrastructure on which the fileshares reside.

[38] During its forensic investigation, eHealth identified that approximately 50 million files were exposed to Ryuk. As noted above, the original metadata scan identified 5.5 million files that potentially contain personal information and/or personal health information. However, the tool developed by eHealth identified 547,145 files that potentially contain

personal information and/or personal health information that may have been infected by the malware. I am not able to conclude exactly how many file were potentially infected by the malware and potentially stolen.

[39] On January 21, 2020, eHealth discovered that files were disclosed to malicious internet protocol (IP) addresses in Germany and the Netherlands. In total, it appears 17 servers and 10 workstations were found to have disclosed data. eHealth's completed Questionnaire detailed that between December 20, 2019 and January 5, 2020, approximately 40 gigabytes (GB) of data was disclosed to three IP addresses – two in Germany and one in the Netherlands. eHealth advised my office that the files that were disclosed were encrypted, therefore, there is no way to know or ever know what data was stolen.

[40] As a result, eHealth cannot definitively conclude that the extracted information contained personal information and/or personal health information. However, as there were at the very minimum 547,145 files containing personal information and/or personal health information exposed to the ransomware (possibly more depending upon the accuracy of the tool developed by eHealth), I must conclude that personal information and personal health information of citizens of Saskatchewan was either exposed to the malware or maliciously stolen from eHealth, the SHA and Health.

[41] eHealth advised my office that the attacker(s) sent reports of encrypted files to several users which were accompanied by ransom demands. eHealth provided my office with a copy of one of the ransom demands it received. In part, the demand stated:

> …You have to pay for decryption in bitcoins. The final price depends on how fast you write to us. Every day of delay will cost you [sic] additional +0.5 BTC….

[42] eHealth did not pay the ransom. Even if eHealth had paid the ransom, there would be no way to know whether or not the malicious actors kept a copy of the data that was stolen.

[43] Although eHealth, the SHA or Health are not able to determine what information was stolen by the malicious actors as the stolen information was encrypted, given the amount of information involved, I must conclude that information containing personal information

and/or personal health information was stolen from eHealth, the SHA and Health. Therefore, the role of my office is to determine if the privacy breach was appropriately handled. In order to be satisfied my office would have to be confident that eHealth, the SHA and Health took the incident seriously and appropriately addressed it.

[44] I find there was privacy breach containing personal information and personal health information.

[45] My office recommends four best practice steps when responding to a privacy breach. These are:

1. Contain the breach;
2. Notification;
3. Investigate the breach; and
4. Prevent future breaches.

[46] Upon completion of these steps, the government institution, local authority or trustee should prepare an internal privacy breach report. Upon notification, my office will request that the government institution, local authority or trustee complete the Questionnaire so my office can conduct its investigation.

[47] I will now consider if eHealth, the SHA and Health appropriately addressed these four best practice steps.

Step 1: Contain the Breach

[48] Upon learning that a privacy breach has occurred, a government institution, local authority or trustee should immediately take steps to contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;

- Revoking access privileges; or
- Correcting weaknesses in physical security.

[49] Effective and prompt containment may reduce the magnitude of a breach and in some instances, the risks to individuals.

[50] As eHealth is the IMSP for the SHA and Health, much of the containment fell on eHealth. However, as the SHA and Health retain custody/possession and control of their information, they cannot shift responsibility of all the containment efforts to eHealth as the IMSP.

[51] Through my office's investigation, it was discovered that there were three critical opportunities – two by eHealth and one by the SHA employee - where the ransomware may have been detected at an early stage. Had these opportunities not have been missed, eHealth may have been able to detect the ransomware, shut down its systems and stopped the extraction of data.

[52] My office discovered each of these opportunities in one of the documents the SHA provided my office as an appendix titled: *[SHA] Investigative Report in the matter of [Employee Name] actions triggering the ransomware attack on the SHR* [sic] *and eHealth IT systems in January 2020* (SHA Investigative Report), dated February 5, 2020. This report included the interview notes and the internal investigation into the SHA employee who brought the ransomware into eHealth, SHA and Health's systems. The SHA Investigative Report was completed by an official with the SHA.

[53] A few bulleted points on page 5 of this report state:

> …
> - Prior to Dec 24 eHealth called [employee name] to log off [their] network and change [their] password. [They] complied.
> - On Dec 24 [they] got a message from [name] at [job search company] indicating, "Dear Colleagues, Unfortunately, my e-mail has been compromised. Please delete all suspicious e-mails from this address. Thanks for your cooperation. Warm Regards. [Name].

- [They] was working from home during Christmas time and [they] was again asked by eHealth to log off the network and change [their] password. [They] complied.

…

[54] First, I will look at the first and third bullet. As the dates in these bullets fell around the same time that the ransomware was first executed on eHealth's system, my office followed up with eHealth to find out why the employee was asked to log off the network and change their password on multiple occasions during that timeframe. As it appeared that the SHA employee was flagged shortly after the ransomware infected the system, my office contacted eHealth for an explanation. eHealth responded to my queries about this potential threat as follows:

> eHealth uses a tool called Advanced Threat Analytics (ATA). This tool alerts technicians of any suspicious activity.
>
> During the week of December 23rd, 2019, the ATA tool generated two alerts focused on the workstation that was the source of the ransomware attack. One of the alerts warned of activity "using an unusual protocol implementation. This may be a result of malicious tools used to execute attacks".
>
> There are normal security protocols which outline steps to be taken when this kind of alert is generated. Both Security and IT Operations officials investigated the alerts, but nothing was found out of the ordinary. The user had been logged onto the workstation for over 6 days so the workstation was remotely shut down and re-started. Since there were no further alerts, no further action was taken.
>
> Looking back on the incident with hindsight, it could perhaps be argued that more rigorous steps were required. However, the ransomware is specifically designed to avoid detection under these circumstances.
>
> Standard protocols are now being revised and enhanced, guaranteeing a more aggressive response when these early signs of suspicious activity are detected.
>
> [Emphasis added]

[55] The early threat was detected by eHealth, however, was not thoroughly investigated at the time. Asking an employee to change their password when there is a background threat is like changing the locks to your door while the burglar is still inside – it's pointless.

[56] In response to the draft report, eHealth offered the following in its defense:

Standard protocols were followed at the time and it is unlikely that the ransomware would have been detected even with a more in-depth investigation. In particular:

- This malware had not previously been identified by anti-virus systems. In fact, this event resulted in a worldwide update to anti-virus software to be able to detect this type of malware.

- At the time, standard procedures were followed. A Ryuk ransomware campaign is a very sophisticated infection that utilizes a three part attack. The initial infection is from a Trojan called Emotet. Emotet uses functionality that helps the software evade detection by anti-malware products and uses worm-like capabilities to move laterally and infect other connected computers and new areas of the network.

- eHealth's Security team uses a tool called Advanced Threat Analytics (ATA) to alert them to suspicious activity. They receive alerts daily. When they receive an alert, they do an initial investigation to determine if it requires further investigation. When further investigation is required, it is sent to IT Operations for follow-up. In this case, activity was detected on the user's workstation under the HEALTHADMIN account. Security followed up with IT Operations to see if they were doing any work under that account. IT Operations investigated and determined everything looked normal with the exception that the user had been logged onto their VDI [virtual desktop infrastructure] session for over 6 days. Security recommended that the session be refreshed so the workstation was shut down. There were no additional alerts received so it was assumed the issue was fixed.

[57] eHealth does not agree that it could have detected the malware based on its comments to the draft report, but the Provincial Auditor of Saskatchewan (Provincial Auditor) has also identified that there are gaps in security monitoring by eHealth.

[58] The Provincial Auditor conducted an audit of eHealth ending August 1, 2019: *Provincial Auditor of Saskatchewan 2020 Report – Volume 1* (Auditor Report – Volume 1), released June 23, 2020. The Provincial Auditor conducted a further audit of eHealth ending March 31, 2020: *Provincial Auditor of Saskatchewan 2020 Report – Volume 2* (Auditor Report – Volume 2), released December 8, 2020.

[59] In section 4.8 of the Auditor Report - Volume 1, the Provincial Auditor commented on eHealth's limited monitoring of unauthorized network access. Pages 61 and 62 of the Auditor Report – Volume 1, in part states:

> 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.
>
> (https://auditor.sk.ca/pub/publications/public_reports/2020/Volume_1/2020%20Report%20--%20Volume%201.pdf, accessed December 2, 2020)

[60] The Provincial Auditor made the following recommendation in the Auditor Report – Volume 1, on page 62 in response to the above:

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

[61] As this recommendation could help enhance eHealth's ability to detect the malicious activity, I will also make this recommendation.

[62] In addition, I recommend that eHealth undertake a comprehensive review of its security protocols to include in-depth investigation when early signs of suspicious activity are

detected. In response to the draft report, eHealth advised it is in the process of engaging an independent, third party vendor to conduct a comprehensive review of its protocols.

[63] I find that eHealth failed in fully investigating the two early threat occurrences, which may have prevented the malicious extraction of data that followed.

[64] The third missed opportunity is outlined in the second bullet in paragraph [53]. The employee had actively been looking for employment with a popular job search company and had been communicating with a legitimate employee with that company. When the SHA employee received the email that contained the ransomware, it appeared as though it was being sent by the job search company employee and looked like it was regarding a legitimate job opportunity. However, when the job search company employee alerted the SHA employee of their email being compromised, the SHA employee did not appear to take any action.

[65] The lack of action of the SHA employee may have been due to the fact they did not receive sufficient training. I will look at that later in this Report.

[66] Unfortunately, at this time, Saskatchewan does not have a provincial privacy law that applies to the private sector as seen in other provinces such as Alberta, British Columbia and Quebec. Therefore, I am not able to further investigate the job site company and its failure to protect its clients more rigorously.

[67] Once the data extraction was discovered, eHealth advised my office it took several measures to stop the unauthorized extraction. These measures can be broken down into the following three phases:

- January 5 – 8, 2020: initial eHealth incident response to limit impact of Ryuk activity;
- January 9 – 17, 2020: Microsoft Detection and Response Team (DART) response; and
- January 17 – March 16, 2020: eHealth's treatment of systems not addressed by DART response.

[68] eHealth further advised that its initial response to the ransomware incident focused on identification of impacts and containment of the threat to prevent impact to its partners' infrastructures and information. This included:

- Isolation of infected computers and file systems under attack;
- Blocking of traffic between eHealth and partner infrastructures;
- Identification of initial attack vectors and agents;
- Identification and termination of ransomware deployment mechanism;
- Identification and complete rebuild of infected core identity infrastructure;
- Identification and mitigation of account credentials primarily used to attack systems;
- Verification and protection of data backup systems; and
- Verification of extent of personal information and personal health information in progress.

[69] On September 29, 2020, eHealth forwarded my office its completed Questionnaire and supporting documents. As of the date of the Questionnaire, eHealth advised that it and its partners continue to address systems untreated by the Microsoft DART response. This includes:

- Remediation/removal of malware threats;
- Verification of anti-malware integrity and functionality; and
- Application of security patches (i.e. supported systems).

[70] As I do not want the contents of this report to put eHealth at risk for another attack, I will not get into the technical details of eHealth's containment efforts.

[71] It appears that eHealth is taking the necessary steps to eradicate the ransomware from its systems and restore the infected data. However, as noted above 40 GB of encrypted data was maliciously stolen from eHealth, the SHA and Health – this is 40 GB of data that will never fully be able to be recovered.

[72] Therefore, all the best measures to stop the practice are overshadowed by the fact that data was stolen and cannot be recovered. The irreparable damage this has caused cannot be undone.

[73] A critical part of eHealth's ongoing attempts to contain the breach is to continue monitoring if the stolen data resurfaces. The most likely place for the data to resurface is on the dark web.

[74] First, I would like to explain the dark web. There are three levels of internet – surface web, dark web, and deep web. The following is a description of each found on the Center for Internet Security's (CIS) website:

- **The Surface Web** is what users access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration, such as Mozilla Firefox, Microsoft's Internet Explorer or Edge, and Google Chrome.

- **The Deep Web** is the portion of the web that is not indexed or searchable by ordinary search engines. Users must log in or have the specific URL or IP address to find and access a particular website or service. Some pages are part of the Deep Web because they do not use common top-level domains (TLDs), such as .com, .gov, and .edu, so they are not indexed by search engines, while others explicitly block search engines from identifying them. Many Deep Web sites are data and content stored in databases that support services we use every day, such as social media or banking websites. The information stored in these pages updates frequently and is presented differently based on a user's permissions.

- **The Dark Web** is a less accessible subset of the Deep Web that relies on connections made between trusted peers and requires specialized software, tools, or equipment to access. Two popular tools for this are Tor and I2P. These tools are commonly known for providing user anonymity. Once logged into Tor or I2P the most direct way to find pages on the Dark Web is to receive a link to the page from someone who already knows about the page. The Dark Web is well known due to media reporting on illicit activity that occurs there. Malicious actors use the Dark Web to communicate about, sell, and/or distribute illegal content or items such as drugs, illegal weapons, malware, and stolen data. However, just like the Surface Web, there are several legitimate activities on the Dark Web as well, including accessing information, sharing information, protecting one's identity, and communicating with others. Many news organizations operate on the Dark Web to protect confidential sources.

  (https://www.cisecurity.org/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web/, accessed on October 30, 2020)

[75] The dark web is best known for illegal and criminal activity that is conducted anonymously.

[76] eHealth advised that on January 21, 2020, it engaged the services of a specialized firm, Hitachi Systems Security though SaskTel, to search and monitor the dark web to see if eHealth, SHA or Health information was being made available and/or for sale.

[77] As of the date of this Report, no eHealth, SHA or Health information has been detected. eHealth advised that it has initiated a second round of dark web monitoring that commenced September 21, 2020.

[78] Janet Burt-Gerrans, Acting Director of Investigations and Mediation, Office of the Information and Privacy Commissioner (IPC) for Nova Scotia, spoke to dark web monitoring and made a recommendation surrounding the length of time to dark web monitor when an employee of the Nova Scotia Health Authority (NSHA) responded to a fraudulent email resulting in the personal health information of 2,841 individuals being compromised:

> [84] The NSHA did not take any steps to further contain the privacy breach. Further steps to contain the breach could take the form of monitoring whether the breached personal health information surfaces on the internet or the dark web or within markets for the sale of personal information. .
>
> …
> [141] **Recommendation #2:** I recommend that beginning immediately, the NSHA monitor whether the personal health information at risk in this privacy breach surfaces on the dark web or within the markets for trading in personal information for a minimum of two years.
>
> (Nova Scotia IPC Review Report 20-02 at pages15 and 25)

[79] In Investigation Report 398-2019, 399-2019, 417-2019, 005-2020, 019-2020, 021-2020, I investigated the October 2019 LifeLabs LP (LifeLabs) cyberattack that resulted in the unauthorized disclosure of personal health information of 93,647 Saskatchewan residents. Paragraphs [87] and [88] state:

> [87] LifeLabs also indicated in its notification emails that it was providing cyber security protection services free of charge to all affected individuals for one year. This includes dark web monitoring and identity theft insurance.

> [88] In Investigation Report 103-2017, I recommended that the trustee provide a minimum of five years credit monitoring to affected individuals following a privacy breach. I recommend that LifeLabs and the SHA provide cyber security protection to affected individuals from Saskatchewan for a minimum of five years.

[80] In the LifeLabs case, cyber security protection included dark web monitoring and identity theft insurance. A key difference between this incident and the LifeLabs breach is that LifeLabs was able to identify whose information that had been breached and was able to provide notification to the affected individuals. In this case, eHealth, the SHA and Health will never fully be able to identify which citizen's information was maliciously stolen.

[81] In 2016, LinkedIn (a social media platform connecting professionals with other professionals and employers), issued a notice of a data breach that was related to a data breach the company experienced in 2012:

> **What happened?**
>
> On May, 17, 2016, we [LinkedIn] became aware that data stolen from LinkedIn in 2012 was being made available online. This was not a new security breach or hack. We took immediate steps to invalidate the passwords of all LinkedIn accounts that we believed might be at risk. These were accounts created prior to the 2012 breach that had not reset their passwords since that breach.
>
> (https://www.linkedin.com/help/linkedin/answer/69603/notice-of-data-breach-may-2016?lang=en, accessed November 2, 2020)

[82] News outlets reported that the hacker was attempting to sell the passwords on the dark web in 2016 for 5 bitcoin, or about $2,200 (https://www.cbc.ca/news/business/linkedin-password-hack-1.3588986, accessed November 2, 2020).

[83] The fact that the LinkedIn data was stolen in 2012, and was found available for sale on the dark web four years later in 2016, demonstrates that the malicious actors do not necessarily try to sell the information immediately. The LinkedIn data breach shows that malicious actors have patience and stolen data can end up on the dark web at any time, even years later.

[84] eHealth has engaged in dark web monitoring, however, has not set a timeframe for how long it intends to continue. I recommend that eHealth continue dark web monitoring for a minimum of five years from the date of this Report. I will speak to identity theft protection later in this Report.

[85] In response to the draft report, eHealth advised it is committed to dark web monitoring and will notify individuals should they become aware of inappropriate activity.

[86] As this breach was caused by ransomware and eHealth is the IMSP for the SHA and Health, the SHA and Health have each deferred to eHealth for any containment efforts undertaken. Although eHealth is an IMSP for the SHA and Health, the SHA and Health still retain possession/custody and control of the personal information and personal health information and have an explicit duty to protect that information under FOIP, LA FOIP and HIPA.

[87] Section 24.1 of FOIP and section 23.1 of LA FOIP share similar language and each provides the explicit duty to protect personal information in the possession or under the control of government institutions and local authorities. Section 24.1 of FOIP provides:

> **24.1** Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[88] Section 16 of HIPA provides the explicit duty to protect personal health information in the custody or under the control of a trustee. Section 16 of HIPA provides:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[89] The SHA and Health cannot place all of the fault on eHealth. Responsibility falls to the SHA and Health to make certain that its IMSPs are meeting the duty to protect under FOIP, LA FOIP and HIPA, as the SHA and Health still retain possession/custody and control of the information. I will look at this further later in this Report.

[90] I find that eHealth, the SHA and Health failed to contain the breach.

Step 2: Notification

[91] It is a best practice to inform affected individuals and my office of breaches in most cases. The following is a list of individuals or organizations that may need to be notified as soon as possible after learning of the incident:

- the organization's privacy officer;
- my office;
- the police, if criminal activity is suspected; and/or
- the affected individuals (unless there are compelling reasons why this should not occur).

[92] Notification to individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. It is best to contact the affected individuals directly.

[93] However, there may be circumstances where it is not possible and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices, media advisories, and advertisements.

[94] Notifications should include the following:

- A description of the breach (a general description of what happened);
- A detailed description of the personal information or personal health information involved;
- Steps taken and planned to mitigate the harm and to prevent future breaches;
- If necessary, advice on actions the individual can take to protect themselves;
- Contact information of an individual within the organization who can answer general questions and provide further information;
- A notice that individuals have a right to complain to my office, including contact information; and
- Recognition of the impacts of the breach on affected individuals and an apology.

[95] eHealth notified my office of this incident on January 6, 2020. Based on what eHealth provided to my office, the following are additional notification efforts taken by eHealth:

- On January 5, 2020 at 7:31p.m., eHealth issued a Major Incident Notification to inform its partners in the health care sector. eHealth notified its partners of a "major incident that started this afternoon and continues through this evening…this incident is related to the spread of a malware attack on our technology services." On January 6, 2020, eHealth updated their partners.

- Once the partners were made aware of the ransomware attack, eHealth began receiving several media inquiries. eHealth's CEO gave several interviews to the media on January 6, 2020.

- eHealth met with the Regina Police Service on January 14, 2020, and a file was opened. As of the date of this Report, I understand there has been no outcome from that investigation.

- eHealth posted a banner on its website on January 6, 2020 informing customers that access to MySaskHealthRecord was currently not available. The banner was updated January 7, 2020, to read:

> eHealth Saskatchewan is aware of ransomware that is impacting services provided by eHealth, and is actively investigating the issue. Some services have been disrupted and may not be available during this time. Access to MySaskHealthRecord has been temporarily disabled. New registrations, as well as returning users logging in, will not be able to access the site.

- eHealth made detailed announcements on its Facebook and Twitter feeds regarding this incident on January 6 and 7, 2020.

[96] eHealth did not discover until January 21, 2020, that encrypted and password protected files were sent to the malicious IP addresses. Therefore, eHealth was unable to determine what individuals may have been affected or what information could have been disclosed. On February 7, 2020, eHealth posted the following ransomware update to its website:

> Ransomware Update
>
> eHealth recently discovered that files from some of its servers had been sent to a number of suspicious IP address [sic]. This came to light as part of normal and ongoing forensic analysis, started in the wake of the January 5th 2020 ransomware attack.
>
> That analysis continues.
>
> The files exchanged were encrypted and password protected by the attacker, making it difficult to determine the exact content of those files. Officials with the Ministry of Health and Saskatchewan's Information and Privacy Commissioner have been informed.
>
> *What we're doing:*
>
> - All files have been restored through back-ups;
> - eHealth will continue its security analysis to determine if any further breaches have occurred;
> - eHealth has retained a specialized security firm tasked with scouring the internet for any signs that confidential information has been compromised;
> - Should it be determined that personal health information has left the organization, the public will be advised.
>
> Until this discovery, eHealth had no evidence that any information had left its control during the ransomware event. Our on-going forensic and restoration efforts brought this new information to light.
>
> We apologize for any concern this has caused to our customers and the people of Saskatchewan.

> eHealth will continue to provide updates, should new information be discovered.
>
> (https://www.ehealthsask.ca/Newspage, accessed November 9, 2020)

[97] From a review of its website, eHealth has not updated its news page regarding this attack since February 2, 2020. In a response to the draft report, eHealth advised it was working with both the SHA and Health on providing a further public notification.

[98] eHealth's statements to the media throughout January 2020, were related to its systems being slowed due to the attack, therefore, it would be utilizing more manual processes. The statements at that time were not related to it also being a victim of ransomware.

[99] The SHA notified my office on March 2, 2020, that its information was also impacted by the ransomware attack. In its completed Questionnaire dated September 30, 2020, the SHA advised my office that it would not be notifying individual patients and would work with eHealth to deliver messaging to the public. My office met with the SHA on October 21, 2020. During that meeting, the SHA identified that it would be undertaking some notification efforts. The SHA also acknowledged that it had taken a long time to get to the notification step.

[100] On December 22, 2020, one year after the ransomware entered the networks, eHealth, the SHA and Health issued a joint news release that provided an update in regards to the malware attack.

[101] eHealth advised my office that Health learned on June 2, 2020, that Health's files had also been exposed to the ransomware. However, Health did not notify my office until September 15, 2020 – over 100 days past learning its files had been exposed.

[102] In its completed Questionnaire sent to my office October 29, 2020 - almost five months after learning it was impacted - Health provided my office the following regarding its notification efforts:

> No, the Ministry has not notified affected individuals nor undertaken a specific strategy to communicate broad notifications.
>
> …
> As of the date of this report, the Ministry has not determined how or what notification will be provided due to the scope of the information and will work with eHealth and the SHA to deliver consistent messaging to the public in the coming weeks.
>
> … the Ministry will be working with eHealth and the SHA to deliver consistent messaging and potential support and guidance to the public in the coming weeks.
>
> …
> The Ministry has not issued any public announcements or media releases to date of any kind….

[103] In June, Health should have immediately issued a news release. I am concerned as to why Health and the SHA took this long to inform the public and why eHealth took this long to provide an update to the public.

[104] I recognize that we are in the middle of a pandemic, however, these notification delays are completely unacceptable. I recommend the SHA and Health take immediate steps to provide mass notification including media releases, newspaper notices, website notices and social media alerts.

[105] If the personal information and/or personal health information of identifiable individuals surfaces on the dark web, eHealth, Health and the SHA should notify the individuals as the information is discovered. In Investigation Report 398-2019, 399-2019, 417-2019, 005-2020, 019-2019, 021-2020, I recommended that LifeLabs and the SHA provide cyber security protection to affected individuals for a minimum of five years. As noted earlier in this Report, cyber security protection included dark web monitoring and identity theft protection. As affected individuals will likely only be identified if their information is found through dark web monitoring, I recommend eHealth, the SHA and Health work together and provide identity theft protection, including credit monitoring, to affected individuals for a minimum of five years from the date an affected individual's information is discovered on the dark web.

[106] I further recommend that eHealth, the SHA and Health consider advising in mass notification efforts that they will provide identity theft protection, including credit monitoring, for up to five years for any concerned citizen who requests it.

[107] In response to the draft report, the SHA advised my office:

> When eHealth notified the public early in 2020, eHealth provided public notification on behalf of the partners. The process of determining what files were affected and the consequences of the incident resulted in a thorough investigation and review by eHealth, the SHA and the Ministry of Health. eHealth developed an approach to review the data that may have been compromised in the malware attack, and we agreed to their approach and worked with them closely during the investigation. This extensive investigation, coupled with the COVID-19 response that has taken many resources, leading to delays in better determining the extent of any privacy breach and the associated required notification. eHealth continues to monitor and scan the internet for any signs that Saskatchewan files have found their way into improper hands. The latest six week scan was completed in November and, to date, there is no evidence to show this has happened.

[108] Although eHealth as IMSP can play a role in notification, the SHA and Health have possession/custody and control of the personal information and personal health information. Therefore, they retain ownership of the notification efforts and need to be involved to ensure their IMSP is doing an appropriate job. In addition, it is a positive that there has been no information found on the dark web, as of yet. However, the LinkedIn privacy breach has taught us that it can be several years before stolen data surfaces.

[109] I find that eHealth has not sufficiently provided notification. Further, I find the SHA and Health have failed in their notification efforts due to the excessive delay in providing notification.

Step 3: Investigate the Breach

[110] Investigating the privacy breach to identify root causes is key in understanding what happened. It is an important step in mitigating the risk of a future breach of a similar nature occurring.

[111] Through the containment efforts of eHealth, it learned that the ransomware was brought into the network by an SHA employee. The SHA Investigative Report detailed the events surrounding the SHA employee receiving a phishing email about a job advertisement on their personal email account on December 20, 2019. The employee attempted to forward the infected email to their work email account, however, it was blocked by email security software and was cautioned by an alert sent to their work email.

[112] The employee had their personal tablet charging by a USB chord on their VDI. The employee opened their personal email on their personal tablet while it was charging. The email contained an infected Microsoft Word document as an attachment. Once the employee opened the document, there was a file transfer from the tablet to the VDI. At that point the ransomware was activated and introduced to eHealth's IT environment.

[113] On December 23, 2019, the same employee received another targeted phishing email about a job advertisement which was blocked from being forwarded to their work email. The employee repeated the same steps of December 20, 2019, where another file transfer of the infected file to the VDI took place again infecting the eHealth network with the ransomware. The ransomware was then activated and it comprised the "healthadmin" account with domain administrative privileges (an account with elevated privileges compared to regular user accounts).

[114] As noted earlier in this Report, the employee was actively looking for employment and the phishing email they received appeared to be from the employee's contact with the job search company – it in fact was the job search company employee email that was first compromised. This created a domino effect resulting in the ransomware being dropped into the networks.

[115] The SHA interviewed the employee that brought the ransomware into the system. From the interview notes, it appears that the employee had received privacy training but did not receive training on the SHA's Acceptable Use of Information Technology (IT) Assets policy. The SHA Investigative Report, in part, concluded the following:

- The employee was not aware of the details of the Acceptable Use of IT assets and had not read the policy [Acceptable Use of IT Assets policy] before the incident;
- The employee opened a corrupt file on their personal device that was charging on a USB connection to their SHA network computer. This is how the corrupt file was introduced into the network causing a ransomware attack;
- The employee did this without the intent to cause harm and with very limited knowledge of how the actions could cause harm; and
- The employee provided a reasonable explanation as to why they believed that the file they were opening was a normal Microsoft Word document related to a job search with a legitimate representative from a well-known job search website. The employee had been actively looking for employment and had found employment from what [they] thought was the same job search website.

[116] Overall the SHA Investigative Report concluded that the employee's actions were not malicious or culpable, but the employee could have taken additional precautions to ensure that the network remained safe from the ransomware attack.

[117] An employee cannot be held culpable if they are not provided appropriate awareness and/or training. In the above bulleted interview notes, the employee advised that they were not aware of details of the Acceptable Use of IT Assets policy. In SHA's completed Questionnaire it noted that the employee admitted they did not have any formal IT security training and that the employee did not follow the Acceptable Use of IT Assets policy.

[118] It is not the employee's responsibility to seek out the policies they are bound by – it is the employer's responsibility to provide training and awareness on any applicable policies. The SHA did not in this case, therefore, the SHA is at fault for not providing training.

[119] I find the SHA did not provide the employee with training on its Acceptable Use of IT Assets policy.

[120] The Provincial Auditor also commented on the lack of training within the SHA in the Auditor Report – Volume 1, on pages 52 and 53:

> …
> In addition, both eHealth and the [SHA] require staff to complete a test on the training received to show their awareness.

> 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. 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 [SHA's] goal is to have 21,900 staff (of it's over 40,000 staff) complete the training by March 31, 2020, and all staff complete the training by March 31, 2021. The [SHA] requires staff to sign a standard Confidentiality Agreement upon being hired; it refers to its security policies and procedures.
>
> eHealth has not asked the [SHA] to place a priority on training [SHA] 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 [SHA] staff completed the training….

[121] The SHA's focus should be getting this number from 50% to 100% of all staff.

[122] The Provincial Auditor made the following recommendation in the Auditor Report – Volume 1, in response to the above on page 53:

> We recommend eHealth Saskatchewan work with the [SHA] to implement an annual security awareness training program for users of portable computing devices with access to the eHealth IT network.

[123] From a review of the SHA's Acceptable Use of IT Assets policy dated and in effect December 4, 2017, it does not speak to charging a personal device on and SHA/eHealth asset. Therefore, even if the employee had been made aware of the policy they actually would not have been in contravention of the policy based upon their actions.

[124] Health did not speak to employee training in its completed Questionnaire, as it was not a Health employee who brought the ransomware into the networks. However, Health did advise in its completed Questionnaire that, "[t]he Ministry does not require eHealth, as IMSP, to have specific training and is unaware of the specific training eHealth employees undergo." Health is entrusting eHealth as an IMSP with sensitive data of this province's

citizens. As such, Health should know and require in its agreement with eHealth that eHealth report on what training eHealth employees have taken and how often the training is refreshed.

[125] eHealth has advised my office that it has completed a tender for procuring cyber security awareness training. Health advised my office that this training would be deployed to the health sector, including Health. eHealth indicated that the training would be deployed in October 2020.

[126] In response to the draft report, eHealth provided my office with the following update related to cyber security training:

- Mandatory cybersecurity training for all eHealth employees was rolled out on November 17, 2020 and was required to be completed by December 15, 2020.
- This training must be completed by eHealth employees yearly and must be completed by new hires within their first 3 days of employment at eHealth.
- Results of the training are tracked in the system and employees must pass a quiz (defined as a score of 70% or greater) to indicate successful completion of the training.
- eHealth is working with its partners to deploy this training more broadly.

[127] eHealth and its partners have been tasked with protecting the provinces most sensitive data. In my opinion, a 70% pass for cyber security training is not a high enough threshold. A pass should be at minimum 90% and ideally 100%.

[128] Therefore, I recommend eHealth review and reconsider the 70% cyber security training pass mark for its employees and its partners' employees and increase the pass mark to a minimum of 90%.

[129] In addition, to ensure that this training proceeds, I recommend eHealth complete the cyber security and privacy training to employees of eHealth, its partners, the SHA and Health by March 31, 2021. Further, I recommend that eHealth require that cyber security and privacy training be required for eHealth and its partners as part of all new employee orientation and

onboarding. Finally, I recommend that all eHealth and eHealth partners be required to complete cyber security and privacy refresher training on an annual basis.

[130] As detailed earlier in this Report, eHealth requested the employee change their password two times within the days following the ransomware infection. There was actually a third instance of the employee being requested to change their password, however, that was on January 7, 2020 – after the malicious file extraction and ransom demands.

[131] As outlined in its completed Questionnaire, eHealth engaged SaskTel to assist in incident response, including a security architect, digital forensics (two employees) and corporate security. In its role, SaskTel prepared an 840 page Digital Forensic Analysis (SaskTel Report/DFA) report. My office was provided a copy of the DFA.

[132] SaskTel's DFA has outlined some very troubling weaknesses in eHealth's network security and network infrastructure. For example, on page 30 of the DFA, SaskTel identified gaps and weaknesses that demonstrate that eHealth's networks are vulnerable. Page 33 of the DFA identifies that eHealth does not even have an accurate list of its servers. In part, page 33 states:

> …Early in this process it became clear that the biggest roadblock to this endeavor was going to be determining an accurate inventory of servers that need to be covered. In the end the team cobbled together as accurate of a list as could be determined and then counted on the network team and others to come to us when other servers were found which needed to be included but did not meet onboarding requirements….

[133] eHealth holds the most sensitive information of the citizens of this province. The fact that eHealth needed to "cobble together" an inventory of servers in order to respond to a ransomware attack is incomprehensible. eHealth delivers IT to our publicly funded healthcare system. Maintaining an inventory of servers is "IT Service Provider 101".

[134] The DFA further criticizes eHealth on page 33:

> …The onboarding proceeded very slowly. It was clear that [eHealth] was extremely cautious about implementing security controls that had not been present previously to the point where it was believed that leaving vulnerable servers on the network

> unprotected [sic] than to implement security controls that could have saved them from an attack. While I get that caution is necessary to protect the business functions, especially in a health care environment, but a better balance needs to be found if eHealth is ever going to mature from a cyber security point of view.
>
> [Emphasis added]

[135] The DFA was also highly critical of eHealth's governance. Page 49 of the DFA stated:

> Currently eHealth is operating in a situation where they have been given a mandate, but they do not have the authority, or the personnel, to influence that mandate. Instead of the various parts of eHealth collaborating to deliver a secure environment you instead find pockets of power which are wielding that power to their own advantage to the detriment of the overall success of the eHealth mandate. Looking at this from a cyber security point of view this has resulted in [sic] hodge podge of unintegrated security solutions being deployed, in various configurations, being operated in various parts of the organization and any attempts to improve the overall security posture of the organization met with resistance and often futility to the point where staff are frustrated and defeatist. This has resulted in inconsistent application of security controls across the organization and even the absence of security controls on many systems including some of the most critical systems in the organization. Dealing with these governance issues will not be easy, and will require a cultural shift at eHealth, but without these changes it is going to be difficult to move forward with cyber security maturity.

[136] In response to my draft report, eHealth provided my office with the following rebut to the SaskTel Report:

> It is important to note that the scope of the SaskTel report was to provide comments from a technical forensic perspective. As such, there is no basis or qualification for the individuals preparing the report to provide comments outside of that scope (e.g. as it relates to eHealth's culture). Further, the comments in the SaskTel report are unverified allegations and opinions based on information obtained from a small group within eHealth. The comments are not factual or reflective of eHealth as an organization. Finally, eHealth and its Executive team members were not given an opportunity to respond to these allegations and opinions.…

[137] eHealth engaged the services of SaskTel and has had the SaskTel Report for months. If eHealth felt it necessary to "respond to the allegations and opinions" of an organization that eHealth retained to undertake the investigation, it had ample time to do so. Further, upon my office's request, eHealth provided me a copy of this report. At the time eHealth

provided my office with the SaskTel Report it did not raise any arguments surrounding the contents of the SaskTel Report.

[138] eHealth should be operating in a cohesive and collaborative manner and not following a governance model which potentially allows for an egocentric and power based approach. This model feeds a chaotic environment where the effective protection of the province's most sensitive data is difficult to fully achieve because those with power in the organization are looking out for themselves.

[139] Unfortunately, eHealth's completed Questionnaire focused on how it technically responded to the breach and data recovery and really lacked the inner soul searching to assess where eHealth fell short and what eHealth could have possibly done to prevent this from happening. For example, eHealth's answer to, "What factors or circumstances contributed to the privacy breach", was:

> Initially the SHA employee's forwarding of the spear-phishing email was blocked, and warned twice by eHealth to "not" complete action. The independent determination of the employee to open the email from [their] personal email account using [their] SHA workstation resulted in the introduction of the Ryuk malware within the eHealth environment. Had policy and procedure been followed in accordance with IT Acceptable Use of Assets Policy, the ransomware exposure would not have occurred.

[140] First of all, the employee was not made aware of the Acceptable Use of IT Assets policy. Secondly, nowhere in eHealth's completed Questionnaire or supporting documentation was there any sort of admission or recognition that eHealth potentially missed two major red flags at a point where the malicious extraction could have possibly been stopped. My office uncovered this important detail in two unassuming sidebar bullets in a report that the SHA provided my office.

[141] As I do not want to compromise eHealth's network security, I will not get into details of network infrastructure and security issues. However, the following points to specific portions of the DFA where SaskTel has recommended changes or enhancements. I am also recommending these changes or enhancements that have been detailed in the SaskTel Report:

- Page 30: Lateral Movement
- Page 49: Increase Cyber-Security Maturity
- Page 50: Security Organization
- Page 50: Incident Response Recommendations

[142] My office does commend eHealth for engaging SaskTel. The DFA was a very comprehensive report that provided my office with important details in order to conduct the investigation.

[143] In response to the draft report from my office, eHealth provided the following to my office:

> It is important to note that cybersecurity breaches occur even on the best protected systems and this should be noted in the Draft Report. Cybersecurity attacks continue to become more sophisticated and protective measures are continuously updated to meet new threats. In this case, the malware had not previously been identified by anti-virus systems and this event resulted in a worldwide update to anti-virus software to be able to detect this type of malware.

[144] I absolutely recognize that organizations are under continued threat of cyber security attacks. As such, the organizations that hold the citizens of this provinces most sensitive data must strive to be the best protected systems with the most thoroughly cyber security trained employees to mitigate the risk of these attacks happening.

[145] I cannot overlook the fact that eHealth had two flags. As noted above and information provided from eHealth:

> One of the alerts warned of activity "using an unusual protocol implementation. This may be a result of malicious tools used to execute attacks".

[146] Based on this, if eHealth had more thoroughly investigated these flags, it could have potentially stopped the ransomware much earlier than it did. The root cause of this breach of privacy was the SHA employee. The SHA failed in providing the employee with the required training. Further, eHealth did not meet its duty to protect the personal information and personal health information of the citizens of this province by not fully investigating the alerts.

[147] Nevertheless, I find that an adequate investigation into this matter was conducted.

Step 4: Prevent Future Breaches

[148] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. Essentially, this is what steps can be taken to prevent a similar privacy breach from occurring. To assist, some questions a government institution, local authority or trustee can ask itself are:

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

[149] In each completed Questionnaire, eHealth, the SHA and Health indicated the following measures were being taken to prevent future breaches.

[150] eHealth advised my office that it had already taken the following preventative measures below. The SHA and Health deferred to eHealth for the preventative measures taken:

- Regular vulnerability scanning of all health system assets in production;
- Dark Web Monitoring;
- Email security upgrade;
- Outbound Internet (white/black list) capability in production with reporting and logging; and
- Forensics investigation.

[151] eHealth and Health advised that the following preventative measures were planned. The SHA deferred to eHealth for the preventative measures taken:

eHealth

- Cybersecurity Awareness Training vendor selection with program deployment;
- Dark Web Monitoring 2nd iteration beginning September 30, 2020;
- Draft "Password Policy", "Stale Account De-activation Policy" and "Outbound Internet (white/black list) Policy";
- Advanced Threat Analytics (ATA) deployment health system wide deployment; and

- Microsoft Defender Advanced Threat Protection (MDATP) deployment to 95% of user assets in production within health system.

Health

The Ministry is currently assessing and planning the following:

- Internal Ministry communication and briefing materials are currently being distributed to senior leaders. Information is being prepared for distribution to all Ministry staff in the coming weeks.

  …
- The Ministry follows, customizes and implements the records management directives of the Government (Archives, ARMS, ORS, etc.). The Ministry is currently in that review and updating process and policy to ensure consistent and appropriate retention, archiving and destruction policies across the Ministry for both paper and electronic records, and the proper controls to manage [personal information]/[personal health information] are in place (i.e. where they are saved, format, naming standards, etc.). We believe this will reduce the amount of information that could be exposed in a similar breach in the future. This is a multi-year project that is in its early phases.
  - The Ministry is currently working with eHealth on password, account and file clean-ups and deletions where applicable. The review and clean-up is 80% complete and anticipated to be complete by end of December.
  - The Ministry is also undertaking a review to document, describe and capture of the depth and breadth of the information on our files shares. It is hoped this work can be completed by year-end.
- The Ministry will be undertaking a thorough review of the IMSP Agreement between the Ministry of Health and eHealth. As noted in the above section on IMSPs, the 2011 IMSP agreement with eHealth needs to be updated and modernized as it does not have strong or detailed technical assurances nor service levels that the Ministry should expect. A more modern and legally sound agreement should be developed.
- The Ministry will be developing a news release or similar statements to be issued to the public. The Ministry plans to work with eHealth and the SHA to develop a common communication strategy to ensure consistent messages are communicated to the public across many platforms; and that messaging builds on what eHealth and the SHA have issued to-date so statements about the incident are consistent and presented as a continuous process.
  - Part of the strategy should address where and how individuals can seek additional support or information.

[152] eHealth has identified the following safeguards that need to be put in place. The SHA and Health deferred to eHealth for safeguards as follows:

eHealth

- Governance, patch and vulnerability management of health system assets in production;
- Disaster Recovery and Business Continuity plan for operational critical assets in production; and
- Health system employees' successful completion of Cybersecurity Awareness Training.

[153] eHealth, the SHA and Health identified the following training requirements:

> **eHealth**
> Yes. Health system employees' successful completion of Cybersecurity Awareness Training, including verification of understanding of IT Acceptable Use of Assets [Policy] and demonstrated competency in identification of (spear) phishing attack.
>
> **SHA**
> The SHA is working with eHealth to provide cybersecurity awareness training to all SHA employees. A vendor has been chosen, and eHealth will work with the SHA to roll it out to SHA employees. Details of the training (training platform, frequency, etc.) are still being developed.
>
> **Health**
> As described in eHealth's Questionnaire, eHealth is planning to provide cybersecurity awareness training to all health sector, including Ministry employees. A vendor has been chosen, and eHealth will work with the Ministry to roll it out to Ministry employees. Details of the training (training platform, frequency, etc.) are still being developed. This will be a good addition to complement the privacy training all Ministry staff and new hires complete.

[154] Finally, eHealth and Health identified the following practices that should stop as they relate to personal information and personal health information. The SHA deferred to eHealth for practices that should stop. Those include:

> **eHealth**
> Yes. In regards to the general protection of [personal information] and [personal health information], eHealth should refrain from the practice of allowing trustees to utilize production data in a test environment through the utilization of existing eHealth data de-identification capability. Work on this is in progress.
>
> **Health**
> A comprehensive review by the Ministry of network file share contents along with development and implementation of a fulsome records retention policy could result in the identification and elimination of unnecessary collection, use, disclosure or retention of [personal information]/[personal health information].

[155] The above steps put forward have not really provided my office with sufficient detail to know if the preventative measures go far enough. Later in this Report, I will discuss quarterly progress updates from eHealth, the SHA and Health, including that of the above preventative measures.

[156] I would now like to discuss additional preventative measures.

[157] Health provided my office with a copy of the IMSP Agreement between Health and eHealth. This agreement was signed by eHealth and Health in April 2011 – almost 10 years ago. The term of the agreement is in effect for an indefinite term, unless terminated by one of the parties with six months notice.

[158] Health addressed the old IMSP agreement in its completed Questionnaire and advised my office of the following:

> With or without an independent assessment, it is noted that a thorough review should be considered and completed by the Ministry of the IMSP Agreement between the Ministry of Health and eHealth. This agreement is dated (2011) and does not have strong or specific technical assurances nor service levels that the Ministry should expect. A more modern and legally sound agreement should be developed.
>
> …
> The Ministry will be undertaking a thorough review of the IMSP Agreement between the Ministry of Health and eHealth. As noted in the above section on IMSPs, the 2011 IMSP agreement with eHealth needs to be updated and modernized as it does not have strong or detailed technical assurances nor service levels that the Ministry should expect. A more modern and legally sound agreement should be developed.

[159] I applaud Health for recognizing the IMSP Agreement should be modernized. However, going forward the IMSP Agreement with eHealth should not include an indefinite term. Technology, security requirements and threats and overall IT needs are changing at lightning speed. Therefore, these agreements should not exceed a three year term and should be reviewed on an annual basis. This will ensure that at least once a year each party turns its attention to the agreement and its contents.

[160] I recommend Health and eHealth's IMSP agreement not exceed a three year term and is reviewed annually. I also recommend that Health and eHealth's current IMSP agreement dated April 2011, be updated and signed within six months of the date of this Report. In response to the draft report, eHealth advised my office that eHealth and the SHA is currently developing a new agreement that will have a three year term and will be reviewed annually. Further, it advised that upon completion of that agreement, a similar agreement will be put in place with Health.

[161] On the other hand, the SHA and eHealth continue their partnership under the interim agreement. In their completed Questionnaires, neither the SHA nor eHealth have addressed finalizing the interim agreement. One facet of finalizing the agreement is to move SHA IT staff to eHealth and moving towards common IT security policies. The Provincial Auditor commented on this in the aforementioned Auditor Report – Volume 1, on page 51:

> 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.
> ...
>
> 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.

[162] Until the SHA IT employees are transitioned to eHealth and a centralized set of policies are put in place, this ad hoc approach leaves eHealth and its partners in a more vulnerable state. In response to the draft report, eHealth advised that this is being considered as part of the agreement between eHealth and the SHA and that the implementation of this agreement contemplates that a centralized set of policies will be rolled out with eHealth's partners.

[163] Later in this Report, I discuss an independent governance, management and program review of eHealth. I recommend that once the governance, management and program review of eHealth is complete, eHealth and the SHA consider the transition of SHA IT employees to eHealth. However, in the interim, I recommend that within six months of the date of this Report, the SHA and eHealth should be following the same set of IT policies and procedures, including the security policies.

[164] In the Auditor Report – Volume 2, the Provincial Auditor commented that an adequate IT Service Level Agreement was still not in place as of November 2, 2020. Pages 29 and 30 of the Auditor Report – Volume 2, states:

> eHealth continues to not have an adequate service level agreement with the [SHA] for the IT services provided. The interim operating agreement effective late 2017 is not adequate.
>
> IT is an integral part of delivering and managing health care services (e.g., lab systems, accounting systems). In January 2017, the Minister of Health directed eHealth to consolidate IT services the [SHA], Saskatchewan Cancer Agency, and 3sHealth previously provided into a single service. At March 31, 2020, this consolidation is not yet complete. eHealth does not have a single set of IT policies or processes and staff within the [SHA] continue to provide IT services.
>
> As of March 31, 2020:
>
> - eHealth and the [SHA] had an IT consolidation committee to help guide the consolidation of IT services into eHealth.
> - eHealth and the [SHA] discussed a draft master service agreement for the provision of IT services but had not finalized it.
>
> Adequate service level agreements make it clear what type of service must be provided, when, and at what cost. They outline in detail services to be provided (e.g., help desk services, server maintenance, frequency of applying patches), service availability requirements (e.g., the percentage of time networks will be available), and service delivery targets (e.g., period for creating and removing user accounts). In addition, they identify security and disaster recovery requirements and set out options available in the event something goes wrong (e.g., data security breach, IT system outage). Agreements also provide a basis for a common understanding and monitoring of performance.
>
> Without an adequate service level agreement, there is a risk that eHealth is not meeting the [SHA]'s IT needs.

> [Emphasis added]
>
> (https://auditor.sk.ca/pub/publications/public_reports/2020/Volume_2/2020%20Report%20--%20Volume%202.pdf, accessed December 9, 2020)

[165] The Provincial Auditor and I are in agreement. Therefore, I recommend that within nine months of the date of this Report the SHA and eHealth sign a finalized IMSP Agreement that adequately addresses IT service delivery.

[166] Malicious actors are discovering new ways every day to trick employees into clicking links and opening documents that contain viruses and malware, including ransomware. In a review of the IT acceptable use policies of eHealth, the SHA and Health, my office found that the policies were very high level documents that did not provide employees with concrete examples of what they should and should not do. IT acceptable use policies and corresponding awareness training should include examples that reflect the most current threats employees should look out for.

[167] Therefore, I recommend IT acceptable use policies of eHealth, the SHA and Health be continually reviewed and amended to include examples of current threats that employees should be aware of. Further, I recommend eHealth, the SHA, and Health develop a strategy to ensure employees are made aware of current threats.

[168] Malicious actors know the best time to hit organizations with ransomware. In the DFA, SaskTel included some background research on this. The March 17, 2020 article by Jai Vijayan, *Many Ransomware Attacks Can Be Stopped Before They Begin* (https://www.darkreading.com/attacks-breaches/many-ransomware-attacks-can-be-stopped-before-they-begin/d/d-id/1337329, accessed December 3, 2020) observed the following:

> Many threat actors tend to lurk around compromised networks for days before deploying ransomware, giving victim organizations a chance to prevent the attacks if they can spot the initial activity quickly enough.
>
> Researchers from FireEye Mandiant recently reviewed more than two years' worth of ransomware attack data to see what trends they could spot. The researchers wanted to

> identify common characteristics around initial intrusion vectors, average attacker dwell time on a compromised network, and the time of day when attackers typically tended to deploy ransomware.
>
> Their study showed that in a majority of incidents, attackers waited at least three days after breaking into a network to identity [sic] key systems to target with their ransomware. Such post-compromise ransomware deployment is growing in popularity because it is often more damaging for victims and more profitable for attackers than other models, says Kelli Vanderlee, manager, intelligence analysis at FireEye.
>
> … the dwell time between initial compromise and ransomware deployment gives organizations a chance to neutralize the attack before it even has a chance to unfold, Vanderlee says. "In most cases ransomware is not executed until days after the initial intrusion, which means it is possible for defenders to prevent ransomware encryption before it starts if they can catch the first signs of activity quickly enough," she says.
>
> …
>
> **Tactical Deployment Strategy**
>
> FireEye's research also showed that in more than three-quarters (76%) of the incidents, attackers deployed the ransomware on a victim network outside normal office hours. Twenty-seven percent of the attacks the security vendor studied happened on weekends. About half (49%) occurred before 8 a.m. or after 6 p.m. on weekdays. Less than a quarter (24%) took place during office hours.
>
> Attackers appear to be favoring off-hours on the assumption that response and remediation would be slower. "When ransomware is executed during business hours, it is more likely that network defenders will be able to respond quickly, potentially stopping the spread of ransomware in a network or preventing additional executions," Vanderlee says.
>
> The trend highlights the need for emergency planning, Vanderlee says. Organizations need to have security technology and staff in place 24/7 in order to catch the first signs of malicious activity. They also need to have clear and redundant escalation plans so that when an incident happens, the correct stakeholders are notified as quickly as possible.…

[169] In this case, the two emails were received December 20, 2019 and December 23, 2019. December 20, 2019 was a Friday and December 23, 2019 was a Monday, two days before Christmas. Although there were two early detection flags, the ransomware lurked around the network throughout Christmas and New Years before it extracted the data. The above article notes, "Organizations need to have security technology and staff in place 24/7 in order to catch the first signs of malicious activity." As eHealth is the IT service provider

for Saskatchewan's health sector, it should review if it has appropriate security technology staff in place 24 hours a day.

[170] If it does not already, I recommend eHealth review whether it should have IT security staff in place 24 hours a day, seven days a week to actively monitor and investigate potential threats. In response to the draft report, eHealth has advised my office it has requested funding from Health for this.

[171] In response to the draft report, the SHA advised my office of the following:

> The SHA would also like to bring to your attention that we have engaged [consulting firm] to assist in a Cyber Governance Assessment to review Current State, Gap Analysis, and provide Recommendations for strengthening the SHA's cyber governance. The assessment involves SHA and the services received from eHealth and includes an environmental scan, documentation review, targeted workshops, and focused Subject Matter Expert interviews in multiple domains related to Cyber Security that cover Policies and Standards, Risk Management, Third Party Security, Awareness and Communications, etc. The report is anticipated in early 2021 and will help inform the creation of a Cyber Program within the SHA as well as SHA requirements in the IT Services Agreement between SHA and eHealth….

[172] The SHA advised my office that the final report and recommendations are expected by the consulting firm in January 2021. This is a great step by the SHA in navigating a path forward.

[173] Earlier in this Report, I discussed the concerns raised by SaskTel in the DFA related to eHealth's governance:

> …Instead of the various parts of eHealth collaborating to deliver a secure environment you instead find pockets of power which are wielding that power to their own advantage to the detriment of the overall success of the eHealth mandate. Looking at this from a cyber security point of view this has resulted in [sic] hodge podge of unintegrated security solutions being deployed, in various configurations, being operated in various parts of the organization and any attempts to improve the overall security posture of the organization met with resistance and often futility to the point where staff are frustrated and defeatist… Dealing with these governance issues will not be easy, and will require a cultural shift at eHealth, but without these changes it is going to be difficult to move forward with cyber security maturity.

[174] Based upon the above, eHealth should review its governance and management structure. Therefore, I recommend that the Minister of Health immediately commence an independent governance, management and program review of eHealth based upon the concerns put forward by SaskTel, the Provincial Auditor and this Report.

[175] I find that although eHealth, the SHA and Health provided my office with some preventative measures, they were not comprehensive or detailed.

[176] I have made several recommendations throughout this Report and there is a lot of work for eHealth, the SHA and Health to complete. Therefore, I recommend that eHealth, the SHA and Health provide my office with a quarterly update of its progress in developing and implementing the preventative measures outlined in this Report. In response to the draft report, eHealth advised my office that it is committed to work with the SHA and Health on this.

[177] This investigation has troubled me in several ways. I am troubled that any citizen of this province that reads this Report could unknowingly have their personal information or personal health information floating around the dark web right now for sale to the highest bidder. I am also troubled that at this moment citizen's data could have been sold to fund criminal activity or purchased by the worst of humankind for nefarious purposes.

[178] Although this investigation has troubled me, I trust that eHealth, the SHA and Health will take the necessary steps as outlined in this Report to ensure they are protecting the personal information and personal health information of the citizens of this province and strive to have the best protected systems with the best cyber security trained employees.

III FINDINGS

[179] I find that there are government institutions, a local authority and trustees involved along with personal information and personal health information of individuals.

[180] I find eHealth is an IMSP for the SHA and Health pursuant to FOIP, LA FOIP and HIPA.

[181] I find there was privacy breach containing personal information and personal health information.

[182] I find that eHealth failed in fully investigating the two early threat occurrences, which may have prevented the malicious extraction of data that followed.

[183] I find that eHealth, the SHA and Health failed to contain the breach.

[184] I find that eHealth has not sufficiently provided notification.

[185] I find the SHA and Health have failed in their notification efforts due to the excessive delay in providing notification.

[186] I find the SHA did not provide the employee with training on its Acceptable Use of IT Assets policy.

[187] I find that an adequate investigation into this matter was conducted.

[188] I find that eHealth has failed its duty to protect the personal information and the personal health information of the citizens of Saskatchewan as a government institution, a trustee and an IMSP for Health, the SHA and eHealth's partners.

[189] I find that the SHA and Health have also failed their duty to protect that same information without having all the necessary checks and balances in place to ensure that eHealth, their IMSP, was not handling their IT service delivery in a deficient manner.

[190] I find that although eHealth, the SHA and Health provided my office with some preventative measures, they were not comprehensive or detailed.

IV RECOMMENDATIONS

[191] Because this breach deals with the most sensitive information of the citizens of Saskatchewan, many of the recommendations below should be worked on right away. Because of the pandemic, demands on the health care system and administrations of vaccines, I am aware that the recommendations will not get acted on as quickly as they should. In the recommendations below, I have recommended certain things be done within three to nine months of receiving this Report. The timelines would be much shorter if it were not for the pandemic. It is still important for officials to begin this work as soon as possible.

[192] I recommend eHealth utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity.

[193] I recommend that eHealth undertake a comprehensive review of its security protocols to include in depth investigation when early signs of suspicious activity are detected.

[194] I recommend that eHealth continue dark web monitoring for a minimum of five years from the date of this Report.

[195] I recommend the SHA and Health take immediate steps to provide mass notification including media releases, newspaper notices, website notices and social media alerts.

[196] I recommend eHealth, the SHA and Health work together and provide identity theft protection, including credit monitoring, to affected individuals for a minimum of five years from the date an affected individual's information is discovered on the dark web.

[197] I recommend that eHealth, the SHA and Health consider advising in mass notification efforts that they will provide identity theft protection, including credit monitoring, for up to five years for any concerned citizen who requests it.

[198] I recommend eHealth review and reconsider the 70% cyber security training pass mark for its employees and its partners' employees and increase the pass mark to a minimum of 90%.

[199] I recommend eHealth complete the cyber security and privacy training to employees of eHealth, its partners, the SHA and Health by March 31, 2021.

[200] I recommend that eHealth require that cyber security and privacy training be required for eHealth and its partners as part of all new employee orientation and onboarding.

[201] I recommend that all eHealth and eHealth partners be required to complete cyber security and privacy refresher training on an annual basis.

[202] I recommend eHealth address the issues detailed under the heading, "Lateral Movement" on page 30 of the SaskTel Report.

[203] I recommend eHealth increase its cyber security maturity to the highest level as recommended by SaskTel as detailed under the heading, "Increase Cyber-Security Maturity" on page 49 of the SaskTel Report.

[204] I recommend eHealth address the issues detailed under the heading, "Security Organization" on page 50 of the SaskTel Report.

[205] I recommend eHealth address the issues and follow the recommendations detailed under the heading, "Incident Response Recommendations" on page 50 of the SaskTel Report.

[206] I recommend Health and eHealth's IMSP agreement not exceed a three year term and is reviewed annually.

[207] I recommend that Health and eHealth's current IMSP agreement dated April 2011, be updated and signed within six months of the date of this Report.

[208] I recommend that once the governance, management and program review of eHealth is complete, eHealth and the SHA consider the transition of SHA IT employees to eHealth.

[209] I recommend that within six months of the date of this Report, the SHA and eHealth should be following the same set of IT policies and procedures, including the security policies.

[210] I recommend that within nine months of the date of this Report the SHA and eHealth sign a finalized IMSP Agreement that adequately addresses IT service delivery.

[211] I recommend IT acceptable use policies of eHealth, the SHA and Health be continually reviewed and amended to include examples of current threats that employees should be aware of.

[212] I recommend eHealth, the SHA, and Health develop a strategy to ensure employees are made aware of current threats.

[213] I recommend eHealth review whether it should have IT security staff in place 24 hours a day, seven days a week to actively monitor and investigate potential threats.

[214] I recommend that the Minister of Health immediately commence an independent governance, management and program review of eHealth based upon the concerns put forward by SaskTel, the Provincial Auditor and this Report.

[215] I recommend that eHealth, the SHA and Health provide my office with a quarterly update of its progress in developing and implementing the preventative measures outlined in this Report.

Dated at Regina, in the Province of Saskatchewan, this 5th day of January, 2021.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner