Chapter 3
eHealth Saskatchewan

1.0 Main Points

This chapter reports the results of the 2019-20 annual audit of eHealth Saskatchewan.

eHealth's 2019-20 financial statements are reliable. During 2019-20, eHealth complied with the authorities governing its activities related to financial reporting and safeguarding public resources. eHealth had, except for certain aspects of its IT security, effective rules and procedures to safeguard public resources in 2019-20.

At March 2020, eHealth did not have an adequate IT service level agreement in place with the Saskatchewan Health Authority, and has not had one for the past three years. Since 2017, eHealth has been mandated to lead IT services for the health sector, which includes the Authority. Adequate service level agreements make it clear what type of service must be provided, when, and at what cost.

In addition, eHealth requires better risk-based processes for controlling IT network access to help mitigate the impact of security breaches, and the extent of breaches. Improved IT network monitoring would also help timely detection of malicious activity. eHealth experienced a ransomware attack during the year. The attack indirectly impacted the accessibility of certain clinical IT systems (e.g., those used by health care professionals) and caused a serious business disruption for the health sector. Although it took time, eHealth was able to successfully recover the IT systems and related data from backups made prior to the attack.

Also, during 2019-20, eHealth made limited progress on testing its IT disaster recovery plans for the 38 IT systems identified as critical to the health sector. Testing recovery plans assures that critical IT systems can be successfully restored within a reasonable time when disasters occur.

In 2019-20, eHealth improved its conflict of interest and procurement practices. Staff completed annual conflict of interest declarations, followed the sole-sourced procurement policies, tracked value-added items on vendor contracts, and properly approved purchases before it received the related goods or services. These improvements help support eHealth achieving best value when making purchases.

2.0 Introduction

2.1 Background

The mandate of eHealth Saskatchewan is to procure, implement, own, operate, and manage the Saskatchewan Electronic Health Record and, where appropriate, other health IT systems.[1,2]

[1] An electronic health record is a private, lifetime record of an individual's medical information providing health care professionals with immediate access to a patient's test results, past treatments, and medication.

[2] Order in Council 734/2010 issued under *The Crown Corporations Act, 1993*.

eHealth is responsible for managing critical IT services used to administer and deliver health care services in Saskatchewan. This includes responsibility for Saskatchewan's electronic health record and health information systems, and IT systems in use at the Saskatchewan Health Authority, Saskatchewan Cancer Agency and 3sHealth. eHealth is the Saskatchewan health sector's primary disaster recovery provider for IT services.

In addition, eHealth manages Saskatchewan's Vital Statistics Registry and health registrations.[3,4]

2.2 Financial Overview

During 2019-20, eHealth had revenues of approximately $146 million of which almost $120 million was grants from the Ministry of Health, and expenses of $145 million. At March 31, 2020, it held tangible capital assets consisting primarily of computer hardware and system development costs with a net book value of $6 million.

Figure 1—Financial Overview

	Budget 2019-20	Actual 2019-20	Actuals 2018-19
		(in millions)	
Grant from the Ministry of Health	$ 113.2	$ 119.6	$ 115.0
Other Revenues	23.5	26.2	26.0
Total Revenue	$ 136.7	$ 145.8	141.0
Operational and Other Expenses	130.2	135.8	132.3
Amortization	10.0	9.4	10.4
Total Expense	$ 140.2	$ 145.2	$ 142.7
Annual Surplus/(Deficit)	$ (3.5)	$ 0.6	$ (1.7)
Total Financial Assets (e.g., due from General Revenue Fund, receivables)		$ 34.5	$ 26.2
Total Liabilities (e.g., accounts payable, obligations under capital lease)		26.3	24.9
Net Financial Assets		$ 8.2	$ 1.3
Tangible Capital Assets		$ 6.0	$ 14.5

Source: Adapted from eHealth Saskatchewan 2019-20 audited financial statements.

3.0 Audit Conclusions

In our opinion, for the year ended March 31, 2020, we found, in all material respects:

- **eHealth Saskatchewan had effective rules and procedures to safeguard public resources except for the matters described below**

[3] The Vital Statistics Registry registers all births, marriages, deaths, stillbirths, legal name changes, and changes of sex designation that occur in Saskatchewan.

[4] Health registration registers new Saskatchewan residents for provincial health coverage and maintains the registry of residents who are eligible for benefits. eHealth Saskatchewan issues health service cards to residents approved for Saskatchewan's basic health coverage.

- **eHealth Saskatchewan complied with the following authorities governing its activities related to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing:**

  eHealth Saskatchewan's governing Orders in Council
  The Crown Corporations Act, 1993
  The Executive Government Administration Act
  The Financial Administration Act, 1993
  The Vital Statistics Act, 2009
  Regulations and Orders in Council issued pursuant to the above legislation

- **eHealth Saskatchewan had reliable financial statements**

We used standards for assurance engagements published in the *CPA Canada Handbook—Assurance* (including CSAE 3001 and 3531) to conduct our audit. We used the control framework included in *COSO's Internal Control—Integrated Framework* to make our judgments about the effectiveness of eHealth's controls.

We focused our audit efforts on the completeness and accuracy of tangible capital assets, the IT service level agreement with Saskatchewan Health Authority, and progress on disaster recovery plan testing of critical IT systems. We evaluated eHealth’s progress towards improving its conflict of interest and procurement processes. We assessed the reasonableness of significant estimates (like accrued payroll and vacation liabilities) at year-end. In addition, we assessed eHealth's IT security controls for the eHealth IT network and financial-related IT systems.

4.0 Key Findings and Recommendations

4.1 Adequate IT Service Level Agreement Not in Place

We recommended eHealth Saskatchewan sign an adequate service level agreement with the Saskatchewan Health Authority. (*2018 Report – Volume 2*; p. 25, Recommendation 1, Public Accounts Committee has not yet considered this recommendation as of November 2, 2020)

Status—Not Implemented

eHealth continues to not have an adequate service level agreement with the Saskatchewan Health Authority 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 Saskatchewan Health Authority, 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 Authority continue to provide IT services.

As of March 31, 2020:

- eHealth and the Authority had an IT consolidation committee to help guide the consolidation of IT services into eHealth.

- eHealth and the Authority 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 Authority's IT needs.

4.2 Disaster Recovery Plans and Testing Incomplete

We recommended eHealth Saskatchewan have an approved and tested disaster recovery plan for systems and data. (*2007 Report – Volume 3*; p. 248, Recommendation 6; Public Accounts Committee agreement January 8, 2008)

Status—Partially Implemented

eHealth has not completed detailed disaster recovery plans nor conducted testing of those plans for its critical IT systems.[5] eHealth has identified 38 critical IT systems.[6]

Effective disaster recovery planning processes require organizations to validate backup of their data periodically. Occasionally, organizations simulate an actual disaster by doing a full restore at the off-site location and check whether backups are fully functional (i.e., disaster recovery test).

During the year, eHealth experienced a disaster. eHealth's IT network was subject to a ransomware attack.

On December 20, 2019, a computer with access to eHealth's IT network was the target of a spear phishing attack.[7] This attack was undetected by eHealth until it led to a ransomware attack on January 5, 2020.[8] Effective IT network monitoring may detect and mitigate the impact of a successful attack on an organization's corporate network (see **Section 4.3** for recommendations to eHealth related to stronger network controls and monitoring).

This attack led to a serious business disruption. It affected the ability of over 40,000 health sector employees to work effectively. eHealth also incurred significant costs to respond to the attack.

[5] Disaster recovery plans outline how to quickly recover from some event that compromises an organization's IT infrastructure (e.g., network).
[6] Since March 31, 2019, eHealth has deemed one IT system previously identified as critical as no longer critical. eHealth continues to work with its health sector partners (e.g., the Saskatchewan Health Authority) to identify all critical IT systems.
[7] Spear phishing is an email or electronic communications scam targeted toward a specific individual or organization.
[8] Ransomware is a form of malware that encrypts an organization's files. The attacker demands a ransom from the organization to restore access to the data upon payment.

eHealth's management indicated eHealth's initial response to the ransomware attack focused on the identification of impacts and containment of the threat to prevent impacts to its IT network, systems and data. These containment measures indirectly impacted the accessibility of certain clinical IT systems (e.g., those used by health care professionals). The ransomware attack encrypted a significant number of servers and data making them unusable. eHealth did not pay a ransom; instead it recovered its systems and related data from back ups made prior to the attack. This recovery took time and made a number of IT systems unavailable for extended periods.

As ransomware attacks are steadily rising and evolving, organizations like eHealth need disaster recovery plans that enable speedy and easy recovery of data from the point of attack.

In early 2020, eHealth began writing a recovery playbook for each critical IT system.[9] At March 31, 2020, eHealth had completed a recovery playbook for seven of the 38 critical IT systems. eHealth did not complete any disaster recovery testing in relation to these 38 IT systems.

Without tested disaster recovery plans, eHealth, the Ministry of Health, and the Authority may not be able to restore their critical IT systems and data (such as the personal health registration system or provincial lab systems) in a timely manner in the event of a disaster. These entities rely on the availability of those systems to deliver time-sensitive health services.

4.3 Stronger Control over eHealth IT Network Needed

As previously reported in the *2020 Report – Volume 1: Chapter 6 eHealth—Securing Portable Computing Devices*, eHealth did not sufficiently control access to the eHealth IT network, evaluate the effectiveness of its network access controls, or effectively monitor network security logs to detect or prevent malicious activity on the eHealth IT network in 2019-20.

See related recommendations in **Figure 2** made in our audit of eHealth's processes to secure portable computing devices used in the delivery of Saskatchewan health services from unauthorized access, which will help strengthen the security of the eHealth IT network.

Figure 2—Recommendations related to Securing Portable Computing Devices

We recommended eHealth Saskatchewan
➢ Implement a risk-based plan for controlling network access to mitigate the impact of security breaches ➢ Utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity

Source: *2020 Report – Volume 1: Chapter 6 eHealth—Securing Portable Computing Devices*
Public Accounts Committee has not yet considered these recommendations as of November 2, 2020.

Controlling IT network access helps mitigate the risk of security breaches, and the extent of breaches. Effective IT network monitoring helps timely detection of malicious activity and mitigate the risks of a successful attack on its corporate network.

[9] A recovery playbook, a document that typically forms part of the overall recovery plan, documents key aspects and recovery steps management must be aware of to enact the recovery plans during a crisis.

4.4 Conflict of Interest, Procurement and Purchasing Processes Improved

During 2019-20, eHealth improved its processes related to declarations of conflict of interest, and its staff followed its established processes related to documenting reasons for sole-sourced purchases, tracking receipt of value-added items, and approving purchases before the receipt of goods and services. See **Figure 3** for details.

These improvements help eHealth promote a culture of actively identifying, declaring, and mitigating conflicts, and achieve best value when making purchases.

Figure 3—Status of Outstanding Recommendations related to Mitigating Conflicts of Interest and Vendor Influence

Outstanding Recommendations	Key Actions Taken in Year Status at March 31, 2020
eHealth Saskatchewan require all staff complete written conflict of interest declarations annually. *(2019 Report – Volume 1, p. 28, Recommendation 1, Public Accounts Committee has not yet considered this recommendation as of November 2, 2020)*	**Implemented –** eHealth's Board approved its Code of Conduct/Conflict of Interest policy June 26, 2019. During 2019-20, all Board members and staff completed a written conflict of interest declaration.
eHealth Saskatchewan follow its policy that requires all sole-sourced procurement decisions have a completed and approved justification form. *(2019 Report – Volume 1, p. 37, Recommendation 5, Public Accounts Committee has not yet considered this recommendation as of November 2, 2020)*	**Implemented –** eHealth had one sole-source purchase in 2019-20. We tested the purchase and found it complied with eHealth's procurement policy and had all the required documentation (e.g., rationale) on file.
eHealth Saskatchewan track value-added items expected and received through vendor contracts. *(2019 Report – Volume 1, p. 38, Recommendation 8, Public Accounts Committee has not yet considered this recommendation as of November 2, 2020)*	**Implemented –** eHealth had only one contract with value-added items in 2019-20. We found eHealth was tracking expected and received value-added items for this contract appropriately.
eHealth Saskatchewan properly approve purchases before it receives the related goods and services. *(2019 Report – Volume 1, p. 39, Recommendation 9, Public Accounts Committee has not yet considered this recommendation as of November 2, 2020)*	**Implemented –** For the sample of 30 payments we tested where physical goods and services were received by eHealth, we confirmed the date staff signed off goods received was before the payment approval date.