Chapter 1
eHealth Saskatchewan

1.0 Main Points

This chapter reports the result of the 2022–23 annual audit of eHealth Saskatchewan. eHealth is the provincial health sector's primary IT service provider, including disaster recovery service provider.

eHealth's 2022–23 financial statements are reliable. During 2022–23, eHealth complied with the authorities governing its activities related to financial reporting and safeguarding public resources. Other than the following areas, eHealth had effective rules and procedures to safeguard public resources for the year ended March 31, 2023.

At March 2023, eHealth did not yet have an adequate IT service level agreement in place with the Saskatchewan Health Authority. eHealth and the Authority have not finalized key aspects (e.g., security and disaster recovery requirements) of the agreement. Adequate service level agreements clearly outline key IT service expectations. Without a clear understanding of expectations and whether they are fulfilled, the Authority's systems may be breached or unavailable.

Additionally, eHealth had disaster recovery playbooks for all 35 critical IT systems identified as critical to the health sector, but had yet to fully complete disaster recovery testing (e.g., full backup restores) for these systems.[1] Testing recovery plans ensures that eHealth can restore critical IT systems in a reasonable time if a disaster occurs.

eHealth also continued to work on controlling access to its IT network and enhancing its network monitoring. Effective network access controls and monitoring helps in preventing and detecting malicious activity timely, such as a successful attack on its network.

2.0 Introduction

2.1 Background

eHealth Saskatchewan's mandate is to procure, implement, own, operate, and manage critical IT services used to administer and deliver provincial healthcare services including Saskatchewan's electronic health record and health information systems, and IT systems in use at the Saskatchewan Health Authority, Saskatchewan Cancer Agency, 3sHealth, and the Ministry of Health.[2,3,4] eHealth also manages Saskatchewan's vital statistics registry and health registrations.[5,6]

[1] A recovery playbook is a document typically part of the overall IT recovery plan documenting key aspects and recovery steps to enact the recovery plans during a crisis. Since early 2020, eHealth began writing a recovery playbook for each critical IT system it manages.
[2] An electronic health record is a private, lifetime record of an individual's medical information providing healthcare professionals with immediate access to a patient's test results, past treatments, and medication.
[3] Order in Council 734/2010 issued under *The Crown Corporations Act, 1993*.
[4] In January 2017, the Minister of Health directed eHealth to consolidate IT services into a single service that the Saskatchewan Health Authority, Saskatchewan Cancer Agency, and 3sHealth previously provided.
[5] The vital statistics registry registers all births, marriages, deaths, stillbirths, legal name changes, and changes of sex designation that occur in Saskatchewan.
[6] eHealth's registration branch registers new Saskatchewan residents for provincial health coverage and maintains the registry of residents who are eligible for benefits. eHealth issues health service cards to residents approved for Saskatchewan's basic health coverage.

2.2 Financial Overview

During 2022–23, eHealth had revenues of approximately $175 million (of which $154 million were grants from the Ministry of Health), and expenses of $167 million. At March 31, 2023, it held tangible capital assets with a net book value of $14 million consisting primarily of computer hardware and software costs.

Figure 1—Financial Overview

	Actual 2022–23	Actual 2021–22
	(in millions)	
Grant from the Ministry of Health	$ 154.4	$ 151.8
Other Revenues	20.2	15.9
Total Revenue	174.6	167.7
Operational and Other Expenses	162.8	144.2
Amortization	4.1	3.9
Total Expense	166.9	148.1
Annual Surplus	$ 7.7	$ 19.6
Total Financial Assets[A]	$ 45.7	$ 38.9
Total Liabilities[B]	18.8	19.4
Net Financial Assets	$ 26.9	$ 19.5
Tangible Capital Assets	$ 14.0	$ 11.4

Source: eHealth Saskatchewan 2022–23 audited financial statements.
[A] Total Financial Assets include due from General Revenue Fund, receivables, etc.
[B] Total Liabilities includes accounts payable, obligations under capital lease, etc.

3.0 Audit Conclusions

In our opinion, for the year ended March 31, 2023, we found, in all material respects:

- **eHealth Saskatchewan had effective rules and procedures to safeguard public resources except for the matters identified in this chapter**

- **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. The control framework

defines control as comprising elements of an organization that, taken together, support people in the achievement of an organization's objectives.

We focused our audit efforts on the following areas:

- The sufficiency of its IT service level agreement with the Saskatchewan Health Authority
- Progress on testing disaster recovery plans for critical IT systems
- The completeness and accuracy of tangible capital assets
- The reasonableness of significant estimates (such as accrued payroll and vacation liabilities)
- eHealth's IT controls over network access, user access, and change management for financial-related IT systems.

4.0 KEY FINDINGS AND RECOMMENDATIONS

4.1 Key Aspects of IT Service Level Agreement Incomplete

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 agreement January 12, 2022)

Status—Partially Implemented

At March 2023, eHealth Saskatchewan and the Saskatchewan Health Authority had yet to finalize remaining key aspects of their master services agreement for IT services.

eHealth became responsible for the majority of the Authority's IT systems when the Authority moved them to eHealth's data centre in 2017–18, and signed an interim operating agreement in 2017. We found the interim agreement to be inadequate in allowing for appropriate monitoring of IT services. eHealth signed a new master services agreement with the Authority in May 2022.

Our review of the new master services agreement found it included a number of key aspects for the delivery of IT services, such as IT service governance, payments and funding, quarterly reporting, and dispute resolution. However, we found eHealth and the Authority have yet to finalize other key aspects of the agreement—disaster recovery, service levels (e.g., response times, system availability), security requirements, and IT change management. **Figure 2** describes the risks associated with these aspects of the master services agreement still undefined.

Figure 2—Risks Associated with Undefined and Unmonitored Aspects of Master Services Agreement

Key Aspect of IT Service Agreement	Associated Risk
Disaster Recovery	Significant IT applications not available when needed, or loss of data in the event of a disaster. At March 2023, eHealth had not completed or tested disaster recovery plans for certain critical IT systems and data of the Authority (e.g., lab system, hospital admissions system). The Authority depends on these IT systems and data to deliver related services.
Service Levels	Inability to determine whether a service provider meets client needs and whether gaps in service exist (e.g., data backups not occurring as expected, expected response times to incident tickets not met).
Security Requirements	Systems and data not adequately secured (e.g., patches not applied in a timely manner).
IT Change Management	Changes to applications may be executed inappropriately, increasing the risk of an adverse effect on the integrity and availability of IT systems and data.

Source: Developed by the Office of the Provincial Auditor of Saskatchewan.

eHealth expects to finalize the remaining key aspects of the master services agreement with the Authority during 2023–24.

IT systems (e.g., lab systems, payroll systems) are an integral part of delivering and managing healthcare services. The Authority depends on its IT data and systems to deliver healthcare services to the public. Not having an adequate service level agreement increases the risk that eHealth fails to meet the Authority's IT needs. This could, in turn, impact the likelihood the Authority's systems are breached or unavailable for long periods of time.

4.2 Disaster Recovery Plan Testing Required

> ***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 Saskatchewan is responsible for 35 critical IT systems—these are critical for the delivery of healthcare in the province. eHealth has completed disaster recovery plans, but has not fully conducted recovery testing of those plans for these critical IT systems.[7] Disaster recovery testing verifies eHealth can successfully implement plans and restore critical IT systems after a disruption or disaster.

As of March 2023, eHealth has disaster recovery playbooks for all 35 critical IT systems, but has yet to fully complete disaster recovery testing (e.g., full backup restores) for these systems.[8] Critical IT systems include patient health information related to diagnostic imaging, drug prescriptions, laboratory results, hospital admissions, and public health records.

[7] Disaster recovery plans outline how to quickly recover from some event that compromises an organization's IT infrastructure (e.g., network).
[8] A recovery playbook is a document typically part of the overall IT recovery plan documenting key aspects and recovery steps to enact the recovery plans during a crisis. Since early 2020, eHealth began writing a recovery playbook for each critical IT system it manages.

During 2022–23, eHealth focused its efforts on developing a five-year Disaster Recovery Roadmap that includes assessing potential risks to IT systems and establishing appropriate measures for recovery (e.g., the total length of time an IT system can be down after a failure or disaster occurs). eHealth management expected to finalize the Roadmap in 2023–24. eHealth needs to begin disaster recovery testing when its Roadmap is complete.

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

Without fully tested disaster recovery plans, eHealth, the Saskatchewan Health Authority, Saskatchewan Cancer Agency, and the Ministry of Health 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. For example, laboratory test results in provincial lab systems provide information to help clinicians provide better and more effective care for their patients, including timely diagnosis of diseases.

As ransomware and cyberattacks 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.[9]

4.3 Better Control Over and Monitoring of eHealth IT Network Needed

While eHealth Saskatchewan continues to make progress toward implementing effective network access controls and improved monitoring of the eHealth IT network, further work is needed.

As **Figure 3** outlines, eHealth has partially implemented two recommendations about its IT network we first made in our *2020 Report—Volume 1*, Chapter 6.[10] We made these two recommendations during our 2019 audit of eHealth's processes for securing portable computing devices and assess eHealth's progress to implement them annually.

Figure 3—Recommendations Related to eHealth's IT Network

Outstanding Recommendations	Status at March 31, 2023 with Key Actions Taken in Year
We recommended eHealth Saskatchewan implement a risk-based plan for controlling network access to mitigate the impact of security breaches. *(2020 Report – Volume 1*, p. 61, Recommendation 6, Public Accounts Committee agreement January 12, 2022*)*	**Partially Implemented** eHealth is working toward centralized Network Access Controls (NAC) for all health sector agencies and network access ports.[11] It planned to pilot NAC in one medium and one large healthcare facility (e.g., hospitals) by March 31, 2023. However, eHealth paused this pilot project during 2022–23 to focus its efforts on data centre network controls. It anticipates completing the NAC pilot project in 2024–25. Controlling IT network access helps to mitigate the risk of security breaches, and the extent of breaches.

[9] In 2019–20, eHealth experienced an IT disaster when its IT network was subject to a ransomware attack. eHealth recovered its systems and related data from backups made prior to the attack.
[10] *2020 Report—Volume 1*, Chapter 6, pp. 47–63.
[11] Network Access Control (NAC) is the process of restricting unauthorized users and devices from gaining access to a corporate network. NAC ensures that only authenticated users and devices that are authorized and compliant with security policies can enter the network. www.fortinet.com/resources/cyberglossary/what-is-network-access-control (19 June 2023).

Outstanding Recommendations	Status at March 31, 2023 with Key Actions Taken in Year
We recommended eHealth Saskatchewan utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity. *(2020 Report – Volume 1,* p. 62, Recommendation 7, Public Accounts Committee agreement January 12, 2022*)*	**Partially Implemented** eHealth is working toward establishing relationships with service providers to help manage the security of various aspects (e.g., end-point detection and response, intrusion prevention system) of the eHealth IT network. eHealth selected one security service provider. It is also in the process of finalizing a statement of work with another security service provider and has an RFP underway for a third provider. It expects these providers will monitor network security on a 24/7 basis and focus on preventing, detecting, analyzing, and responding to cybersecurity incidents. Without effective IT network monitoring, eHealth may not detect malicious activity and mitigate risks of a successful attack on its corporate network within sufficient time to prevent a security breach.

Source: *2022 Report—Volume 2*, Chapter 15, *eHealth—Securing Portable Computing Devices.*

eHealth 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.