Chapter 1
eHealth Saskatchewan

1.0 Main Points

This chapter reports the results of the 2023–24 annual audit of eHealth Saskatchewan. eHealth is the provincial health sector's primary IT service provider, including disaster recovery service provider.

eHealth's 2023–24 financial statements are reliable. During 2023–24, 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, 2024.

At March 2024, 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 vulnerable to security breaches or be unavailable.

Further, eHealth had disaster recovery playbooks for all 52 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 confirms whether eHealth can restore critical IT systems in reasonable time when a disaster occurs.

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 the provincial electronic health record and health information systems, as well as IT systems in use at the Saskatchewan Health Authority, Saskatchewan Cancer Agency, 3sHealth, and the Ministry of Health.[2,3] eHealth also manages Saskatchewan's vital statistics registry and health registrations.[4,5]

eHealth is the provincial health sector's primary disaster recovery provider for IT services.

[1] A disaster recovery playbook is a document typically part of an overall IT recovery plan documenting key aspects and recovery steps to take during a crisis.
[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] The vital statistics registry registers all births, marriages, deaths, stillbirths, legal name changes, and changes of sex designation that occur in Saskatchewan.
[5] eHealth's registration branch registers new Saskatchewan residents for provincial health coverage and maintains the registry of residents eligible for benefits. It also issues health service cards to residents approved for basic health coverage.

2.2 Financial Overview

During 2023–24, eHealth had revenues of approximately $193 million (of which $168 million were grants from the Ministry of Health), and expenses of $186 million. At March 31, 2024, it held tangible capital assets with a net book value of $22 million consisting primarily of IT hardware and software costs.

Figure 1—Financial Overview

	Actual 2023–24	Actual 2022–23
	(in millions)	
Grant from the Ministry of Health	$ 168.0	$ 154.4
Other Revenues	24.5	20.2
Total Revenue	192.5	174.6
Operational and Other Expenses	182.1	162.8
Amortization	3.7	4.1
Total Expenses	185.8	166.9
Annual Surplus	$ 6.7	$ 7.7
Total Financial Assets[A]	$ 52.4	$ 45.7
Total Liabilities[B]	30.1	18.8
Net Financial Assets	$ 22.3	$ 26.9
Tangible Capital Assets	$ 22.1	$ 14.0

Source: eHealth Saskatchewan 2023–24 audited financial statements.
[A] Total Financial Assets include due from General Revenue Fund, receivables, etc.
[B] Total Liabilities include accounts payable, obligations under capital lease, etc.

3.0 Audit Conclusions

In our opinion, for the year ended March 31, 2024, 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.**

  We also completed a follow-up audit related to eHealth securing portable computing devices, which included assessing two recommendations impacting eHealth's control of its IT network beyond March 2024—neither of these recommendations were fully implemented at March 31, 2024.[6] We report the results of this follow-up audit in Chapter 17 of this Report.

- **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**

[6] In our *2020 Report – Volume 1*, Chapter 6, we recommended eHealth implement a risk-based plan for controlling network access to mitigate the impact of security breaches, and utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity.

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 eHealth's 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 IT Service Level Agreement Not Yet Finalized

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 2024, eHealth Saskatchewan and the Saskatchewan Health Authority had yet to finalize remaining key aspects of their service level agreement for IT services. eHealth has provided IT services to the Authority since 2017.

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 both agencies signed an interim operating agreement in 2017. eHealth signed a new master services agreement with the Authority in May 2022.

Our review of the new master services agreement found it included several 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 Aspects of Master Services Agreement Undefined and Unmonitored

Key Aspect of IT Service Agreement	Associated Risk
Disaster Recovery	Significant IT systems not available when needed, or loss of data in the event of a disaster. At March 2024, 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 healthcare services.
Service Levels	Inability to determine whether a service provider meets client needs and whether gaps in service exist (e.g., 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). Unpatched systems contain known vulnerabilities prone to exploitation.
IT Change Management	Changes to IT systems may be inappropriately executed, increasing the risk of an adverse effect on the integrity and availability of IT systems and data.

Source: The Office of the Provincial Auditor of Saskatchewan.

The Authority paid eHealth $14.9 million for its IT services in 2023–24. An effective service agreement outlines clear expectations, responsibilities, and deliverables for both parties involved in the service relationship. Clarity helps prevent misunderstandings and disputes, and safeguards both parties.

eHealth management indicated they expect to finalize the remaining key aspects of the master services agreement with the Authority during 2024–25.

IT is an integral part of delivering and managing healthcare services (e.g., lab systems, accounting systems). 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.

4.2 Disaster Recovery Plan Testing Still 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 Saskatchewan is responsible for 52 critical IT systems—these are critical for the delivery of healthcare in Saskatchewan. At March 2024, eHealth had not fully tested disaster recovery plans for those 52 critical IT systems.

eHealth has tested aspects of its disaster recovery plans; however, it has not conducted full testing of those plans for the 52 critical IT systems.[7] Disaster recovery testing verifies plans can be implemented successfully and critical IT systems can be restored after a

[7] Disaster recovery plans outline how to quickly recover from an event that compromises an organization's IT infrastructure (e.g., network).

disruption. If a disaster recovery plan does not work as expected, it can lead to extended periods of downtime, which can be costly and disruptive to healthcare services.

As of March 2024, eHealth has disaster recovery playbooks for all 52 critical IT systems (2023: 35 systems).[8] eHealth completed 36 partial tests (e.g., recover a component of a system from backup) and 10 tabletop tests of IT system disaster recovery playbooks.[9] However, eHealth has not completed any full disaster recovery testing. A full disaster recovery test confirms users can log in and demonstrates the system works as expected, in a crisis scenario and within the expected amount of downtime. eHealth has not determined expected downtime (i.e., recovery time objectives) for all 52 critical IT systems as of March 2024, and tested whether recovery time objectives are realistic.

Effective disaster recovery planning processes require periodic validation of data backups. Occasionally, organizations simulate an actual disaster by doing a full restore at an off-site location and check whether backups are fully functional and systems work as expected (i.e., full disaster recovery test).

Without 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 agencies rely on the availability of those systems to deliver time-sensitive health services. For example, doctors require laboratory test results from the provincial lab systems to help provide more effective patient care, including timely diagnosis and treatment.

As ransomware and cyberattacks steadily rise and evolve, agencies like eHealth need disaster recovery plans that enable speedy and easy recovery of systems and data from the point of attack.

[8] A disaster recovery playbook is a document typically part of an overall IT recovery plan documenting key aspects and recovery steps to take during a crisis.
[9] A tabletop test assesses an organization's readiness to respond to cybersecurity incidents by testing if individuals know what to do, who to contact, and communication chains are in place.