

# Chapter 1

## eHealth Saskatchewan

### 1.0 MAIN POINTS

This chapter reports the results of the 2024–25 annual audit of eHealth Saskatchewan. eHealth is the provincial health sector’s primary IT service provider, including for disaster recovery services.

eHealth’s 2024–25 financial statements are reliable. During 2024–25, 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, 2025.

eHealth is responsible for 55 critical IT systems—these are critical for the delivery of healthcare in Saskatchewan. At March 2025, eHealth completed partial testing of disaster recovery plans for these systems, but needs to formally track and complete testing of all system components and aspects of plans to confirm sufficiency of disaster recovery plans. Testing recovery plans confirms whether eHealth can restore critical IT systems in reasonable time when 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.

Also, during 2024–25, eHealth finalized the remaining key aspects (e.g., security, disaster recovery requirements) of its IT service level agreement with the Saskatchewan Health Authority.

### 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.<sup>1,2</sup> eHealth is the provincial health sector’s primary disaster recovery provider for IT services.

eHealth also manages Saskatchewan’s vital statistics registry and health registrations.<sup>3,4</sup>

<sup>1</sup> 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.

<sup>2</sup> Order in Council 734/2010 issued under *The Crown Corporations Act, 1993*.

<sup>3</sup> The vital statistics registry registers all births, marriages, deaths, stillbirths, legal name changes, and changes of sex designation that occur in Saskatchewan.

<sup>4</sup> 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 2024–25, eHealth had revenues of approximately \$224 million (of which \$198 million were grants from the Ministry of Health), and expenses of \$214 million. At March 31, 2025, it held tangible capital assets with a net book value of \$26 million consisting primarily of IT hardware and software.

**Figure 1—Financial Overview**

	Actual 2024–25	Actual 2023–24
	(in millions)	
Grant from the Ministry of Health	\$ 197.9	\$ 168.0
Other Revenues	25.9	24.5
<b>Total Revenue</b>	<b>223.8</b>	<b>192.5</b>
Operational and Other Expenses	208.2	182.1
Amortization	5.9	3.7
<b>Total Expenses</b>	<b>214.1</b>	<b>185.8</b>
<b>Annual Surplus</b>	<b>9.7</b>	<b>6.7</b>
Total Financial Assets <sup>A</sup>	41.3	52.4
Total Liabilities <sup>B</sup>	17.4	30.1
<b>Net Financial Assets</b>	<b>23.9</b>	<b>22.3</b>
<b>Tangible Capital Assets</b>	<b>\$ 25.7</b>	<b>\$ 22.1</b>

Source: eHealth Saskatchewan 2024–25 audited financial statements.

<sup>A</sup> Total Financial Assets include due from General Revenue Fund, receivables, etc.

<sup>B</sup> Total Liabilities include accounts payable, accrued salaries and benefits, etc.

## 3.0 AUDIT CONCLUSIONS

In our opinion, for the year ended March 31, 2025, 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 Saskatchewan'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
- The impact on controls and financial information associated with eHealth's June 2024 implementation of the Administrative Information Management System (AIMS) for processing payroll

## 4.0 KEY FINDINGS AND RECOMMENDATIONS

### 4.1 IT Service Level Agreement 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**—Implemented

In September 2024, eHealth Saskatchewan and the Saskatchewan Health Authority finalized the remaining key aspects of their master service level 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. Both agencies signed the first version of a new master services agreement in May 2022 and the final version in September 2024.



Our review of the September 2024 agreement found it appropriately considered key aspects for the delivery of IT services, such as IT governance, disaster recovery, service levels (e.g., response times, system availability), security requirements, IT change management, payments and funding, regular reporting, and dispute resolution.

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. Having an adequate service level agreement decreases the risk that eHealth fails to meet the Authority's IT needs and reduces the likelihood the Authority's systems are breached or unavailable for long periods.

## 4.2 Disaster Recovery Plans Partially Tested

***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 55 critical IT systems (2024: 52 systems), which are critical for the delivery of healthcare in Saskatchewan. At March 2025, eHealth completed partial testing of disaster recovery plans for these systems, but still needs to formally track and complete testing of all system components and aspects of plans to confirm their sufficiency.<sup>5</sup>

eHealth tested elements of its disaster recovery plans; however, it has not conducted full testing of those plans for the 55 critical IT systems. Disaster recovery testing verifies plans can be implemented successfully and critical IT systems can be restored after a 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 2025, eHealth has disaster recovery playbooks for all 55 critical IT systems.<sup>6</sup> eHealth completed one full test, 43 partial tests (e.g., recovered a system component from backup), and six tabletop tests of IT system disaster recovery playbooks.<sup>7</sup> A full disaster recovery test confirms users can log in and proves the system works as expected in a crisis scenario within the amount of expected downtime. eHealth is working on updating the expected downtime (i.e., recovery time objectives) for all 55 critical IT systems as of March 2025.

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 for users (i.e., full disaster recovery test).

<sup>5</sup> Disaster recovery plans outline how to quickly recover from an event that compromises an organization's IT infrastructure (e.g., network).

<sup>6</sup> A disaster 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.

<sup>7</sup> A tabletop test assesses an organization's readiness to respond to cybersecurity incidents by testing whether individuals know what to do, who to contact, and communication channels are in place.

eHealth indicated that annual full disaster recovery tests may not always be feasible for all 55 systems (e.g., full system outages may negatively impact patient care). It plans to use a risk-based approach to complete partial tests in non-production environments for all 55 critical systems. Partial tests can be less disruptive and useful for testing specific components of systems and plans. However, eHealth has yet to summarize all the system components it has partially tested to demonstrate it has covered all necessary components and aspects of the recovery plans for the 55 critical systems. eHealth expects to begin tracking its partial tests by 2026–27.

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 agencies rely on the availability of those systems to deliver time-sensitive health services. For example, doctors require laboratory test results from 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 tested disaster recovery plans that enable speedy and easy recovery of systems and data from the point of attack.

### 4.3 Better Control 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 2** outlines, eHealth partially implemented two recommendations regarding its IT network we first made in 2020.<sup>8</sup> We made these two recommendations during our 2019 audit of eHealth’s processes for securing portable computing devices and annually assess eHealth’s progress to implement them.

**Figure 2—Recommendations Related to eHealth’s IT Network**

Outstanding Recommendations	Status at March 31, 2025, with Key Actions Taken in Year
<p><b><i>We recommended eHealth Saskatchewan implement a risk-based plan for controlling network access to mitigate the impact of security breaches.</i></b></p> <p><i>(2020 Report – Volume 1, p. 61, Recommendation 6; Public Accounts Committee agreement January 12, 2022)</i></p>	<p><b>Partially Implemented</b></p> <p>eHealth is working toward centralized Network Access Controls (NAC) for all health sector agencies and network access ports.<sup>A</sup> It expects to complete an IT network roadmap in 2025–26 to help guide its implementation of network access controls in 2026–27.</p> <p>Without adequate security on network access ports, the eHealth IT network may be vulnerable to attack through these open ports. Unnecessary, open ports can provide a point of entry for an intruder to gain unauthorized access to a network. Controlling IT network access helps to mitigate the risk of security breaches, and the extent of breaches.</p>

<sup>8</sup> *2020 Report—Volume 1, Chapter 6*, pp. 47–63.



Outstanding Recommendations	Status at March 31, 2025, with Key Actions Taken in Year
<p><b><i>We recommended eHealth Saskatchewan utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity.</i></b></p> <p><i>(2020 Report – Volume 1, p. 62, Recommendation 7; Public Accounts Committee agreement January 12, 2022)</i></p>	<p><b>Partially Implemented</b></p> <p>eHealth began using a service provider in May 2023 to help monitor and manage the security of its IT network—it expects the service provider to monitor network security 24/7 and focus on preventing, detecting, analyzing, and responding to cybersecurity incidents.</p> <p>At March 31, 2025, the service provider had yet to implement network monitoring tools for all expected aspects of the eHealth IT network (e.g., servers) and had not started reporting on its monitoring activities of the eHealth IT network.</p> <p>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.</p>

<sup>A</sup> 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](http://www.fortinet.com/resources/cyberglossary/what-is-network-access-control) (23 June 2025).

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.