Chapter 1
eHealth Saskatchewan

1.0 Main Points

This chapter reports the results of the 2021–22 annual audit of eHealth Saskatchewan.

eHealth's 2021–22 financial statements are reliable. During 2021–22, 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, 2022.

At March 2022, eHealth did not have an adequate IT service level agreement in place with the Saskatchewan Health Authority. eHealth and the Authority signed a new master services agreement in May 2022, but continue to work together on finalizing key aspects of the agreement (e.g., security and disaster recovery requirements). Adequate service-level agreements make it clear what type of service must be provided, when, and at what cost.

eHealth continued to make progress on testing its IT disaster recovery plans for the 35 IT systems identified as critical to the health sector. It completed recovery playbooks and conducted tabletop simulation exercises for all 35 critical IT systems, but did not fully complete disaster recovery testing for these systems (e.g., test restoration of backups).[1] Testing recovery plans assures that critical IT systems can be successfully restored within a reasonable time when disasters occur.

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 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.[5,6]

[1] 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.
[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*, created the agency.
[4] In January 2017, the Minister of Health directed eHealth to consolidate IT services into a single service that the Authority, Saskatchewan Cancer Agency, and 3sHealth previously provided. eHealth also hosts IT systems used at the Ministry of Health.
[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 2021–22, eHealth had revenues of approximately $168 million (of which $152 million were grants from the Ministry of Health), and expenses of $148 million. At March 31, 2022, it held tangible capital assets with a net book value of $11.4 million consisting primarily of computer hardware and system development costs.

Figure 1—Financial Overview

	Budget 2021–22	Actual 2021–22	Actual 2020–21
	(in millions)		
Grant from the Ministry of Health	$ 137.2	$ 151.8	$ 138.2
Other Revenues	23.8	15.9	17.9
Total Revenue	161.0	167.7	156.1
Operational and Other Expenses	154.3	144.2	142.4
Amortization	6.0	3.9	4.4
Total Expense	160.3	148.1	146.8
Annual Surplus	$ 0.7	$ 19.6	$ 9.3
Total Financial Assets [A]		$ 38.9	$ 28.3
Total Liabilities [B]		19.4	21.6
Net Financial Assets		$ 19.5	$ 6.7
Tangible Capital Assets		$ 11.4	$ 11.2

Source: eHealth Saskatchewan 2021–22 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, 2022, we found, in all material respects:

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

  We also completed a follow-up audit related to securing portable computing devices. The follow-up audit includes assessing two recommendations that impact eHealth's control of its IT network—neither of these recommendations were fully implemented at March 31, 2022.[7] We report the results of this follow-up audit in Chapter 15 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**

[7] We made two recommendations about eHealth's IT network 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 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 (like accrued payroll and vacation liabilities)
- eHealth's IT controls over network access, and 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 2022, eHealth and the Saskatchewan Health Authority were nearing completion of a new master services agreement for IT services. eHealth signed the new master services agreement with the Authority in May 2022, and expects to finalize the remaining key aspects of the agreement by March 31, 2023.

eHealth has been responsible for the majority of the Authority's IT systems since 2017–18, and signed an interim operating agreement with the Authority in 2017. We found the agreement to be inadequate to allow for appropriate monitoring of IT services. As of March 31, 2022, eHealth's consolidation of IT services was not yet complete. eHealth does not have a single, comprehensive set of IT policies or processes; and staff within the Authority continue to provide IT services.

Our review of the draft 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 continue to work together on finalizing 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 undefined aspects of the master services agreement.

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

Key Undefined Aspect of IT Service Agreement	Associated Risk
Disaster Recovery	Significant IT applications unavailable when needed, or loss of data in the event of a disaster. At March 2022, 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 is meeting client needs and whether gaps in service exist (e.g., data backups not occurring as expected, expected response times to incident tickets unmet).
Security Requirements	Systems and data inadequately secured (e.g., patches not applied in a timely manner).
IT Change Management	Changes to applications may be inappropriately executed, 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.

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, increase the likelihood the Authority's systems are breached or unavailable for long periods of time.

4.2 Incomplete Testing of Disaster Recovery Plans

> ***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 is responsible for 35 critical IT systems—these are critical for the delivery of healthcare in Saskatchewan. eHealth has completed disaster recovery plans, but has not fully conducted recovery testing of those plans for these 35 critical IT systems.[8]

As of March 2022, eHealth completed a recovery playbook and conducted a tabletop simulation exercise for all 35 critical IT systems.[9,10] However, eHealth did not complete any

[8] Disaster recovery plans outline how to quickly recover from some event that compromises an organization's IT infrastructure (e.g., 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. Since early 2020, eHealth began writing a recovery playbook for each critical IT system.
[10] The tabletop exercise is a meeting to discuss a simulated emergency situation. Members review and discuss the actions they would take in a particular emergency, testing their emergency plan in an informal, low-stress environment.

further disaster recovery testing in relation to these 35 critical IT systems (e.g., full backup restores).

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. [11] These entities rely on the availability of those systems to deliver time-sensitive health services. For example, laboratory test results found in provincial lab systems provide information to help doctors provide better and more effective care for their patients, including timely diagnosis of diseases.

Effective disaster recovery planning processes require organizations to periodically validate backups of their data. 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).

As ransomware attacks are steadily rising and evolving, organizations (like eHealth) need fully tested disaster recovery plans that enable speedy and easy recovery of data from the point of attack.[12]

[11] At March 2022, eHealth's list of 35 critical systems does not include systems from 3sHealth.
[12] 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.