Chapter 3
eHealth Saskatchewan

1.0 Main Points

This chapter reports the results of the 2020–21 annual audit of eHealth Saskatchewan.

eHealth's 2020–21 financial statements are reliable. During 2020–21, 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 2020–21.

At March 2021, eHealth did not have an adequate IT service level agreement in place with the Saskatchewan Health Authority. eHealth began drafting a master service agreement during the year, however it still lacks a number of key provisions. 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 its 35 IT systems identified as critical to the health sector. It completed a recovery playbook for 14 of those critical IT systems, as well as conducted a tabletop simulation exercise on four of the 14 completed playbooks. Testing recovery plans assures that critical IT systems can be successfully restored within a reasonable time when disasters occur.

eHealth improved its risk-based processes for controlling IT network access to help mitigate the extent and impact of security breaches by updating its security threat risk assessment process and installing a new network monitoring tool; however, further work remains. Effective IT network access controls and monitoring helps in the timely detection of malicious activity to mitigate risks of a successful attack on its network.

2.0 Introduction

2.1 Background

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

eHealth is responsible for managing critical IT services used to administer and deliver healthcare services in Saskatchewan. This includes responsibility for Saskatchewan's electronic health record and health information systems, and since 2017, IT systems in use at the Saskatchewan Health Authority, Saskatchewan Cancer Agency and 3sHealth.[3]

[1] 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.
[2] Order in Council 734/2010 issued under *The Crown Corporations Act, 1993*, established eHealth Saskatchewan.
[3] 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 separately.

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.[4,5]

In 2020–21, an integrated IT Advisory Committee formed. The Committee includes representatives from eHealth and various health sector clients, including the Saskatchewan Health Authority. It assists in guiding the strategic priorities for IT services that eHealth is to provide. The Committee met almost monthly throughout 2020–21.

2.2 Financial Overview

During 2020–21, eHealth earned approximately $156 million (of which the Ministry of Health provided $138 million in grants) in revenue, and incurred $147 million in expenses. At March 31, 2021, it held tangible capital assets with an $11 million net book value consisting primarily of computer hardware and system development costs.

Figure 1—Financial Overview

	Actual 2020–21	Actual 2019–20
	(in millions)	
Grant from Ministry of Health	$ 138.2	$ 119.6
Other Revenues	17.9	26.2
Total Revenue	156.1	145.8
Operational and Other Expenses	142.4	135.8
Amortization	4.4	9.4
Total Expense	146.8	145.2
Annual Surplus	$ 9.3	$ 0.6
Total Financial Assets [A]	$ 28.3	$ 34.5
Total Liabilities [B]	21.6	26.3
Net Financial Assets	$ 6.7	$ 8.2
Tangible Capital Assets	$ 11.2	$ 6.0

Source: eHealth Saskatchewan 2020–21 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, 2021, we found, in all material respects:

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

[4] The vital statistics registry registers all births, marriages, deaths, stillbirths, legal name changes, and changes of sex designation that occur in Saskatchewan.
[5] Health registrations register new Saskatchewan residents for provincial health coverage and maintain 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. 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. We assessed eHealth's IT controls over user access, network access, and change management for financial-related IT systems, the sufficiency of its IT service level agreement with the Saskatchewan Health Authority, and its progress on testing the disaster recovery plan for critical IT systems. We examined eHealth's process to grant and revoke health card coverage through its three-year renewal process where December 31, 2023 coverage stickers were sent to eligible Saskatchewan residents in 2020. We also assessed the completeness and accuracy of tangible capital assets, and the reasonableness of significant estimates (like accrued payroll and vacation liabilities).

4.0 Key Findings and Recommendations

4.1 IT Service Level Agreement Progressing

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 October 29, 2021*)*

Status—Partially Implemented

As at March 2021, eHealth and the Saskatchewan Health Authority continued to manage IT services provided to the Authority under an inadequate agreement. During 2020–21, eHealth began drafting a master services agreement for IT services, but we found insufficient provisions at March 2021.

We found the operating agreement eHealth and the Authority signed in 2017 to be inadequate to allow for appropriate monitoring of IT services. eHealth has been responsible for the majority of the Authority's IT systems since 2017–18. As of March 31, 2021,

eHealth's consolidation of IT services 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.

Further, our review of the draft master services agreement found it did not include provisions for a number of key aspects for the delivery of IT services. For example, it did not include provisions about IT change processes, service levels (e.g., response times, system availability), security requirements, and disaster recovery. It appropriately included details on IT service governance, an IT service catalogue, payments and funding, quarterly 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 inadequate service level agreement increases the risk that eHealth fails to meet 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.[6] eHealth is responsible for 35 critical IT systems—these are critical for the delivery of healthcare in Saskatchewan.[7]

As of March 2021, eHealth completed a recovery playbook for 14 of its 35 critical IT systems.[8] During the year, eHealth conducted a tabletop simulation exercise on four of the 14 completed playbooks.[9]

Effective disaster recovery planning processes require organizations to periodically validate backup 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).

eHealth did not complete any disaster recovery testing in relation to these 35 critical IT systems.

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

[6] Disaster recovery plans outline how to quickly recover from some compromising event affecting an organization's IT infrastructure (e.g., network).
[7] Since March 31, 2020, eHealth deemed one additional IT system as critical and four previously identified IT systems as no longer critical. eHealth continues to work with its health sector partners (e.g., Saskatchewan Health Authority) to identify all critical IT systems.
[8] 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.
[9] 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.

In 2019–20, eHealth experienced a disaster. eHealth's IT network was subject to a ransomware attack. eHealth recovered its systems and related data from backups made prior to the attack. 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.

4.3 Better Control Over and Monitoring of eHealth IT Network Needed

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

As **Figure 2** outlines, eHealth partially implemented two recommendations about its IT network we first made in our *2020 Report—Volume 1, Chapter 6*. We made these recommendations during our 2019 audit of eHealth's processes for securing portable computing devices.

Figure 2—Recommendations Related to eHealth's IT Network

Outstanding Recommendations	Status at March 31, 2021 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 has not yet considered this recommendation as of October 29, 2021*)*	**Partially Implemented** eHealth made the following improvements for controlling network access to mitigate the impact of security breaches: ➢ eHealth approved a new password policy and two-factor authentication for remote users.[A] ➢ eHealth updated its Security Threat Risk Assessment process to assess, detect, and repair any security risk associated with network devices. However, eHealth had not completed its IT threat and risk assessment or begun scanning systems for vulnerabilities. eHealth is developing strategies for exerting control over access and permissions for users, accounts, processes, and systems across the IT environment. For example, it plans to review privileged user access in 2021. Setting an appropriate level of privileged access helps agencies condense their attack surface and mitigates damage from attacks.
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 has not yet considered this recommendation as of October 29, 2021*)*	**Partially Implemented** eHealth installed a new network monitoring tool in April 2020. This monitoring tool generates alerts about potential malicious activity. eHealth sets a severity impact rating for alerts, and expects staff to investigate high-rated alerts first. eHealth plans to start a Security Operations Centre to allow for 24/7 real-time security monitoring of its IT network.

Source: *2020 Report—Volume 1, Chapter 6, eHealth—Securing Portable Computing Devices*.
[A] Two-factor authentication is an electronic authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (e.g., key fob and password).

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.