

## Chapter 7

### eHealth Saskatchewan

#### 1.0 MAIN POINTS

This chapter reports the results our audits of eHealth Saskatchewan (eHealth) for the years ended March 31, 2013 and March 31, 2014.

eHealth's 2013 and 2014 financial statements are reliable. It complied with the authorities governing its activities related to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing, and it had effective rules and procedures to safeguard public resources except for three areas.

eHealth needs to follow its processes to remove unneeded user access to its information technology (IT) systems and data promptly. It also needs a complete and tested disaster recovery plan, and needs to authorize all requests for changes to its accounting records on a timely basis.

#### 2.0 INTRODUCTION

Cabinet established eHealth Saskatchewan (eHealth) through an Order in Council under *The Crown Corporations Act, 1993*.<sup>1</sup> The mandate of eHealth is to lead the provincial planning and strategy for the Saskatchewan electronic health record (EHR). Its mandate is also to procure, implement, own, operate, and manage the EHR and other health information systems (e.g., the associated provincial components and infrastructure) to facilitate improved access to health providers and patients and the use of electronic health information. Also, eHealth is responsible for establishing the provincial health information and technology standards necessary to provide access to the Saskatchewan EHR, and the associated provincial components and infrastructure.<sup>2</sup>

eHealth provides the Ministry of Health and the regional health authorities with some critical IT services and operates a data centre. The Ministry's business continuity plan indicates eHealth is its prime disaster recovery provider.

In 2013-14, eHealth had revenues of \$78.6 million (2013: \$104.7 million) including \$67.8 million of grants from the Ministry of Health (2013: \$91.5 million), expenses of \$91.7 million (2013: \$94.2 million) and an annual deficit of \$13.1 million (2013: surplus of \$10.5 million). At March 31, 2014, it had net financial assets of \$11.9 million (2013: \$17.6 million) and tangible capital assets of \$44.8 million (2013: \$51.9 million). Most of its tangible capital assets relate to computer network hardware and system development costs.

<sup>1</sup> Saskatchewan Health Information Network (SHIN) was established as a Treasury Board Crown Corporation by Order in Council 581/1997. SHIN was renamed eHealth Saskatchewan by Order in Council 734/2010.

<sup>2</sup> *Saskatchewan Provincial Budget 14-15 Estimates*, p.167.



## 3.0 AUDIT CONCLUSIONS AND SCOPE

In our opinion, for the years ended March 31, 2013 and 2014:

- › eHealth's financial statements are reliable
- › eHealth had effective rules and procedures to safeguard public resources except for the matters described in this chapter
- › eHealth complied with the following authorities governing its activities related to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing:

eHealth's governing Orders in Council  
*The Crown Corporations Act, 1993*  
*The Financial Administration Act, 1993*  
*The Tabling of Documents Act, 1991*  
Regulations and Orders in Council issued pursuant to the above legislation

We used the control framework developed by the Canadian Institute of Chartered Accountants 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.

In our 2013 and 2014 audits, we examined the effectiveness of eHealth's financial-related controls used to administer the revenues, expenses and assets identified in **Section 2.0**. eHealth's significant expenses include professional fees, software maintenance, and amortization of tangible capital assets. Also, we examined the effectiveness of the controls it used to keep reliable financial records and prepare reliable financial reports.

## 4.0 KEY FINDINGS AND RECOMMENDATIONS

In this section, we outline key observations from our assessments and the resulting recommendations.

### 4.1 Timely Removal of User Access to IT Systems and Data Needed

While eHealth has established processes to promptly remove unneeded user access to its IT systems and data, staff did not consistently follow them.

In our testing of 2013-14 activity, we found 2 out of 13 individuals no longer employed by eHealth had access to its systems and data up to eight months after their last day of employment.

If unneeded access to systems and data is not removed promptly, it increases the risk of inappropriate access to eHealth's systems and data and could result in inappropriate use or manipulation of data.

1. We recommend that eHealth Saskatchewan follow its processes to remove unneeded user access to its IT systems and data promptly.

## 4.2 Changes to Accounting Records Need Timely Approval

We recommended that eHealth approve all requests for changes to accounting records (journal entries) before changing its accounting records. (2012 Report – Volume 2; Public Accounts Committee has not yet considered this recommendation)

**Status** – Partially Implemented

eHealth requires management to review and approve all journal entries. However, during our audits, we found that journal entries were not reviewed and approved on a timely basis.

Lack of timely review and approval increases the risk of fraud and errors without timely detection.

## 4.3 Compliance with Information Technology Security Policies

We recommended that eHealth Saskatchewan follow its policies when disposing of information technology and communication equipment. (2012 Report – Volume 2; Public Accounts Committee has not yet considered this recommendation)

**Status** – Implemented

During our audit, we did not find any incidents of non-compliance with eHealth's policies for disposing of IT and communication equipment.

## 4.4 Disaster Recovery Plan Needed

We recommended that eHealth have an approved and tested disaster recovery plan for systems and data. (2007 Report – Volume 3; Public Accounts Committee agreement January 8, 2008)

**Status** – Not Implemented



eHealth continues to not have a complete and tested disaster recovery plan (DRP). Its DRP does not address the Ministry of Health's and regional health authorities' requirements for recovery of their systems and data located in eHealth's data centre. The ability of the Ministry and regional health authorities to recover their systems and data depends on the adequacy of eHealth's recovery plan.

Without such a plan, eHealth, the Ministry and the regional health authorities may not be able to restore their IT systems and data in the event of a catastrophic IT event at eHealth's data centre.