Chapter 54 Saskatoon Regional Health Authority—Protecting IT Infrastructure

1.0 Main Points

This chapter describes our follow-up of management's actions on five recommendations we initially made in our *2010 Report – Volume 2*, Chapter 11D on Saskatoon Regional Health Authority's (Saskatoon RHA) processes to protect its information technology (IT) infrastructure.

To support the delivery of healthcare services, Saskatoon RHA uses IT systems. For example, it uses IT systems for lab results, medical imaging, and patient registration and billing. It also stores confidential patient data in its IT systems. Its IT systems and data reside on its network and computer equipment. Therefore, maintaining the security of its IT infrastructure is very important to ensure that information from the systems is accurate and timely, and patient data is protected.

We found that management has implemented two of the recommendations and made progress towards the remaining three recommendations. Saskatoon RHA needs to do the following so that it can protect its IT infrastructure. It needs to finish implementing its monitoring controls over its IT infrastructure and have staff follow its established processes for updating its network equipment and removing user access promptly.

2.0 Introduction

This chapter describes our follow-up of management's actions on five recommendations we made in our *2010 Report – Volume 2*, Chapter 11D on Saskatoon RHA's processes to protect its information technology infrastructure. Our *2012 Report – Volume 2*, Chapter 49 reported that by August 2012 Saskatoon RHA had implemented one recommendation and was working towards implementing the remaining five recommendations.

To conduct this review engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate Saskatoon RHA's progress towards meeting our recommendations, we used the relevant criteria from the original audit. Saskatoon RHA's management agreed with the criteria in the original audit.

We interviewed Saskatoon RHA's staff, examined IT policies, reviewed reports about the implementation status of the IT policies, analyzed information from IT systems, and observed IT processes.

3.0 Status of Recommendations

This section sets out each recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of the recommendation at September 30, 2014, and Saskatoon RHA's actions up to that date. We found that Saskatoon RHA has implemented two recommendations and made progress in implementing three recommendations, but still has some work to do.

3.1 IT Policies Implemented

> We recommended that Saskatoon Regional Health Authority implement adequate information technology policies. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)
>
> **Status** – Implemented

Saskatoon RHA has developed, approved, and implemented IT policies to effectively manage its IT infrastructure.

3.2 Monitoring of Security Improving

> We recommended that Saskatoon Regional Health Authority monitor the security of its information technology infrastructure. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)
>
> **Status** – Partially Implemented

Saskatoon RHA approved policies for monitoring access to and use of IT systems and for managing IT security incidents. It completed work to lock and monitor access to all rooms that store its computer equipment. It began implementation of a central logging system to collect IT security data and is evaluating the potential use of additional systems to collect further data. It hired an employee in October 2014 to focus on monitoring IT security to detect security attacks or potential breaches by analyzing the data from these systems.

Saskatoon RHA needs to complete its implementation of monitoring controls for IT infrastructure so that it can timely detect and address security attacks and potential breaches.

3.3 Configuration and Updating of Computer Equipment Improving

> We recommended that Saskatoon Regional Health Authority configure and update its computers and network equipment to protect them from security threats. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)
>
> **Status** – Partially Implemented

Saskatoon RHA has taken steps to improve the configuration of its computer systems and network equipment to protect them from external threats.

In July 2014, Saskatoon RHA implemented a process to update (i.e., patch) its servers semi-annually. It has assessed approximately 41% of the servers to determine what work is required to fully update the equipment. Saskatoon RHA plans to assess and apply updates to the remaining servers by the end of 2015. Based on its assessments completed by September 30, 2014, it reported that it had:

- Updated 28% of its servers
- Decommissioned 7% of its servers
- Accepted risks, in alignment with industry standards, from not updating 4% of its servers
- Assessed, but is working to update 2% of its servers
- Has not assessed or applied updates for 59% of its servers

Although Saskatoon RHA had processes for updating its network equipment (e.g., firewalls, routers), staff did not consistently follow them. At September 30, 2014, we found that some network equipment was not up to date (i.e., patched).

Failure to update computers and network equipment on a timely basis increases the risk of unauthorized access or changes to Saskatoon RHA's systems or data.

3.4 Need to Restrict User Access

We recommended that Saskatoon Regional Health Authority adequately restrict access to information technology equipment, systems, and data. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)

Status – Partially Implemented

Although Saskatoon RHA had processes to grant and remove user access, staff did not consistently follow them. The RHA employs about 15,000 individuals. We analyzed a listing of all users and found 92 individuals no longer employed by the RHA who continued to have access to its systems and data. For example, we found one individual who had access for about six months after the individual left the employ of the RHA.

Continued access of employees who no longer work for Saskatoon RHA increases the risk of unauthorized access or changes to its systems and data.

3.5 Disaster Recovery Plan Approved

We recommended that Saskatoon Regional Health Authority prepare and test an information technology disaster recovery plan. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)

Status – Implemented

In October 2013, Saskatoon RHA completed its first test of its disaster recovery plan and updated its plan based on the test results. In April 2014, it approved the revised plan.