Chapter 48
Prince Albert Parkland Regional Health Authority—IT Security Follow Up

1.0 Main Points

In this chapter, we report the results of our follow-up on the recommendations from our 2011 Report – Volume 1 where we audited Prince Albert Parkland Regional Health Authority's (PA Parkland's) controls to secure its information technology (IT) systems and data.

PA Parkland needs to do more to fully address two outstanding recommendations from our 2011 IT security audit. PA Parkland needs to monitor its data centre, secure wiring closets and encrypt portable computers, and test its disaster recovery plan.

2.0 Introduction

In 2011, we audited PA Parkland's controls to secure (i.e., protect the confidentiality, integrity, and availability) its IT systems and data. We reported the results of our audit in Chapter 11 of our 2011 Report – Volume 1 and made three recommendations for PA Parkland to help improve its processes.

3.0 Status of Recommendations

This section sets out the three recommendations and PA Parkland's progress up to August 31, 2012. PA Parkland has implemented one of our recommendations and needs to do more to fully address the other two recommendations.

3.1 Monitoring Service Providers

We recommended that the Prince Albert Parkland Regional Health Authority monitor whether its information technology service providers meet its security requirements. (2011 Report – Volume 1; Public Accounts Committee agreement August 28, 2012)

Status – Implemented.

At May 31, 2012, PA Parkland ended its contract with its private sector service provider and took over the support and maintenance of its IT data centre. PA Parkland continues to have a service level agreement with eHealth Saskatchewan.[1] Management is working to update its agreement with eHealth including addressing disaster recovery requirements.

[1] eHealth Saskatchewan is a Treasury Board Crown Corporation previously called Saskatchewan Health Information Network.

3.2 Restrict Physical Access

We recommended that Prince Albert Parkland Regional Health Authority restrict physical access to information technology systems and data. (2011 Report – Volume 1; Public Accounts Committee agreement August 28, 2012)

Status – We continue to make this recommendation.

PA Parkland still needs to monitor its data centre, secure its wiring closets, and encrypt portable computers. It has improved its controls over physical access. It has a card reader for its data centre and manually records entries to the facility. It is also beginning a process to receive and review logs of data centre entry. However, PA Parkland still permits maintenance personnel unescorted access to the data centre. PA Parkland does not have any additional controls, such as video monitoring, in place to monitor such unescorted access in the data centre.

PA Parkland does not lock all wiring closets that permit access to network equipment or encrypt portable computers. PA Parkland plans to address these matters by March 31, 2013.

3.3 Maintain and Test Disaster Recovery Plan

We recommended that Prince Albert Parkland Regional Health Authority maintain an up-to-date and tested disaster recovery plan based on a threat and risk assessment. (2011 Report – Volume 1; Public Accounts Committee agreement August 28, 2012)

Status – We continue to make this recommendation.

PA Parkland has not fully documented its recovery procedures and tested its disaster recovery plan.

PA Parkland has developed an approved disaster recovery plan, identified critical systems, and the timelines required to recover them. However, it does not have documented procedures and responsibilities for recovery of those critical systems.

The disaster recovery plan is untested. PA Parkland informally tested some emergency response processes due to an extended power outage in Prince Albert in the summer 2012. However, the testing of emergency response processes did not include recovery of servers and systems or data that reside on the servers. Also, PA Parkland has a number of critical systems that are hosted at eHealth and does not have a process to ensure eHealth can address its disaster recovery requirements. PA Parkland is working towards updating its agreement with eHealth.