# Chapter 52
# Prince Albert Parkland Regional Health Authority—IT Security

## 1.0 Main Points

At March 31, 2014, Prince Albert Parkland Regional Health Authority (PA Parkland) had implemented one of the two outstanding recommendations we made in 2011 related to securing its information technology (IT) systems and data. However, it needs more work to fully implement the second recommendation.

PA Parkland completed a disaster recovery plan and conducted testing as required by its risk assessment. PA Parkland plans to restrict access to its IT wiring closets in rural locations and encrypt all its portable computers by March 31, 2015.

## 2.0 Introduction

PA Parkland is responsible for the planning, organization, delivery, and evaluation of health services in its health region. PA Parkland uses IT systems and data for admissions, patient records, laboratory results, prescription information, and accounting. Its IT systems collect, store, and process information, including confidential information, used for treatment of individuals and for planning and decision making at both the regional and provincial levels. Securing PA Parkland's IT systems and data is important for safe and effective delivery of health services and protection of patient information.

Our *2011 Report – Volume 1* reported that PA Parkland needed to restrict physical access to its IT systems and data, maintain and test its disaster recovery plan, and monitor whether its IT service providers meet its security requirements. We made three recommendations. By August 31, 2012, as reported in our *2012 Report – Volume 2*, PA Parkland had addressed one recommendation, but needed to do more to address our other two recommendations. This chapter reports the results of our second follow-up on the remaining two recommendations.

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

We assessed PA Parkland's activities since our last follow-up to March 31, 2014 related to restricting physical access and disaster recovery planning. We also assessed the adequacy of PA Parkland's current disaster recovery plan and reviewed the results of its 2014 testing of recovery procedures.

## 3.0 Status of Recommendations

This section sets out each outstanding recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of

the recommendation at March 31, 2014, and PA Parkland's actions up to that date. We found PA Parkland had addressed one of our remaining recommendations, but still had some work to do to address the other one.

## 3.1 Working to Adequately Restrict IT Wiring Closets and Portable Computers

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** – Partially Implemented

PA Parkland installed video cameras to monitor its data centre. This, along with its other controls to restrict physical access (i.e., use of card reader, and the manual recording of those who enter the data centre), is sufficient to restrict physical access to its data centre.

However, at March 31, 2014, PA Parkland's controls to restrict physical access to its IT wiring closets[1] and portable computers needed strengthening. PA Parkland has about 40 IT wiring closets and 300 portable computers located throughout the region. Staff use portable computers to access health information.

Not adequately securing physical assess to wiring closets and portable computers increases the risk of unauthorized access to sensitive data. Management advised that PA Parkland plans to address these matters by March 31, 2015.

## 3.2 Disaster Recovery Plan Complete

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** – Implemented

PA Parkland conducted a business impact analysis to determine the importance of the IT systems used in its health region. PA Parkland completed a disaster recovery plan,[2] which includes fully documented procedures for its network, server, and system recovery. In addition, PA Parkland conducted disaster recovery testing as required by its risk assessment.

[1] Wiring closets are small rooms that house critical IT network infrastructure (e.g., switches, wires). They are located outside of the centralized server room or data centre.
[2] A disaster recovery plan is a plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is often part of a larger, organization-wide business continuity plan.