Prince Albert Parkland Regional Health Authority

11

Main points

Prince Albert Parkland Regional Health Authority (PA Parkland) uses information technology systems and data for admissions, treatment records, laboratory results, prescription information, and finances. PA Parkland has two main service providers managing its systems and data.

The objective of this audit was to assess whether PA Parkland had adequate processes to secure (i.e., protect the confidentiality, integrity, and availability of) its information technology systems and data for the period August 1, 2010 to January 31, 2011.

We concluded that for the period August 1, 2010 to January 31, 2011, PA Parkland had adequate processes to secure (i.e., protect the confidentiality, integrity, and availability of) its information technology systems and data except for the following. To protect its systems and data, PA Parkland needs to monitor whether its service providers meet its security requirements. It should also restrict physical access to its systems and data and maintain and test its disaster recovery plan. Physical access controls protect computers and network devices from unauthorized access and disaster recovery plans ensure systems and data are available when needed.

Introduction—Securing IT systems and data

The Prince Albert Parkland Regional Health Authority (PA Parkland) is responsible for the planning, organization, delivery, and evaluation of health services in its health region. PA Parkland, with 2,400 employees, is responsible for providing health services to the region's population of 78,000 people at an annual cost of about $181 million.[1]

Information technology (IT) has become a key tool in managing and delivering health services. PA Parkland uses IT systems and data for admissions, treatment records, laboratory results, prescription information, and finances. IT systems collect, store, and process information, including confidential information, used for treatment of individuals and for planning and decision making at the regional and provincial level.

Securing PA Parkland's systems and data is of fundamental importance for safe and effective delivery of health services and protection of patients' interests. Use and protection of IT will become even more important as electronic health records are implemented in Saskatchewan.

PA Parkland uses two main service providers to manage its systems and data. One service provider is an agency of the Ministry of Health; the other service provider is a private sector company. PA Parkland must oversee the security provided by these service providers.

Inadequate security of IT systems and data increases the risk that patients' medical records could be lost, inaccurate, compromised, or not available when needed, resulting in incorrect decisions and mistakes in patient care. Inadequate security could also lead to inappropriate disclosure of patients' medical records.

Audit objective, criteria, and conclusion

The objective of this audit was to assess whether the Prince Albert Parkland Regional Health Authority had adequate processes to secure (i.e., protect the confidentiality, integrity, and availability of) its information

[1] *Prince Albert Parkland Regional Health Authority 2009-2010 Annual Report* (pp.5, 32, 34).

technology systems and data for the period August 1, 2010 to January 31, 2011.

To conduct this audit, we followed the *Standards for Assurance Engagements* published in the *CICA Handbook - Assurance*. To evaluate PA Parkland's processes, we used criteria based on the *Trust Services Principles, Criteria, and Illustrations*, international standards, and literature and reports of other legislative auditors (see the selected references). PA Parkland agreed with the criteria in Exhibit 1.

Exhibit 1—Audit criteria

To have adequate controls to secure (i.e., protect the confidentiality, integrity, and availability) its information technology systems and data, we expect Prince Albert Parkland RHA to:

1. **Show management commitment to security**
   - Responsibility for security is clearly defined
   - IT planning supports security
   - Management has approved security policies and procedures
   - Management monitors security including service providers
2. **Protect systems and data from unauthorized access**
   - User access controls protect the systems and data from unauthorized access
   - Physical security controls protect against unauthorized access
3. **Keep systems and data available for operation**
   - System and data backups occur and are tested
   - Disaster recovery plans are in place and are tested
4. **Maintain the integrity of systems and data**
   - Change management processes exist and are followed
   - Computer operation processes exist and are followed

We concluded that for the period August 1, 2010 to January 31, 2011, the Prince Albert Parkland Regional Health Authority had adequate processes to secure (i.e., protect the confidentiality, integrity, and availability of) its information technology systems and data except for its processes to:

- **Monitor whether its information technology service providers meet its security requirements**
- **Adequately restrict physical access to information technology systems and data**
- **Maintain and test its disaster recovery plan**

Key findings and recommendations

We describe below what we expected (in italics) and our key findings for each criterion together with our recommendations.

Show management commitment to security

Management commitment includes setting up an organizational structure that clearly defines who is responsible for security. We expected PA Parkland would have a member of senior management lead the IT division. We expected PA Parkland to have an approved IT strategic plan. Commitment also includes implementing and monitoring compliance with security policies and procedures. We expected management would effectively monitor service providers who perform work on its behalf.

PA Parkland has an appropriate organizational structure for IT, including leadership by members of senior management. The IT area has experienced significant change but PA Parkland's IT strategic plan does not reflect the impact of this change. Management told us that it plans to update its IT strategic plan.

PA Parkland has adequate IT security policies and procedures. To deliver IT services and help manage security, PA Parkland makes significant use of two service providers. PA Parkland has adequately documented security requirements with one of the service providers. PA Parkland needs to ensure it agrees on security requirements with both. PA Parkland does not receive sufficient security reports from its service providers or routinely use quality assurance or third party assessments that would allow it to assess the security of the services provided. Weaknesses at the security providers could adversely affect the security of PA Parkland's systems and data.

1. We recommend that the Prince Albert Parkland Regional Health Authority monitor whether its information technology service providers meet its security requirements.

Protect systems and data from unauthorized access

We expected PA Parkland to have adequate physical access and user access processes to protect its systems and data from unauthorized access.

Good physical control means protecting IT infrastructure from harm. Physical access controls protect all computers and network devices from unauthorized access. For example, a locked door could physically prevent unauthorized users from accessing a server room.

User access controls ensure only approved people or processes can use an IT system. A common example of a user access control is a username and a password. The username identifies the user and the password grants access.

Protecting systems from unauthorized access is more critical with the increased use of the Internet, automated processes, and multiple locations. PA Parkland should protect its data by configuring, updating, and monitoring its systems against security threats.

PA Parkland needs to improve its physical access controls. PA Parkland secures its data centre with locked doors. However, it permits a large number of employees to have physical access to the data centre. PA Parkland monitors who has physical access to the data centre and uses video surveillance in the area of the entrance to the data centre. PA Parkland does not lock all wiring closets that permit access to network equipment.

PA Parkland does not require encryption of portable computers. This increases the risk of unauthorized access to sensitive information if a portable computer is lost or stolen. PA Parkland has provided employees with portable USB memory devices that offer encryption. However, PA Parkland did not provide employees with training on how to use the devices securely. We found sensitive data unencrypted on such a device. Management told us that it intends to secure its portable computers and restrict the use of USB memory devices.

2. We recommend that the Prince Albert Parkland Regional Health Authority restrict physical access to information technology systems and data.

PA Parkland has procedures to grant, modify, and remove user access to its computers and network. PA Parkland uses its service providers to manage access. PA Parkland did not consistently notify its service providers on a timely basis to remove user access to its network and data (e.g., for terminated employees). By the end of the audit period, PA Parkland was providing timely reports to the service providers to help ensure that user access was appropriate.

PA Parkland has established policies with one of the service providers to help protect its systems and data from unauthorized access. The service provider has configured equipment to enforce the agreed-upon rules. The service provider updated PA Parkland's servers and network equipment for known weaknesses on a timely basis.

The service provider also maintains the firewall that protects PA Parkland's data centre. The service provider monitors the firewall and alerts PA Parkland when necessary.

Keep systems and data available for operation

We expected PA Parkland to have adequate processes to ensure its systems and data are available for operation when needed.

Even with good backup and recovery procedures, PA Parkland might not be able to continue its operations if a major problem occurred. Therefore, we expected PA Parkland to have a contingency plan to recover operations in the event of a disaster like a fire or flood. This includes building capacity into systems, when cost effective, so a disaster in one location will not cause applications to quit running at other locations where employees are still able to work.

PA Parkland has adequate environmental controls (e.g., for temperature changes) for its data centre. These controls assist in preventing damage to the data centre.

PA Parkland uses one of the service providers to back up its data. Backed up data is kept at a location outside the health region. This assists in keeping data available for operation, particularly in the event of a local disaster.

PA Parkland has developed a disaster recovery plan. The plan contains information to assist PA Parkland in coping with an interruption in its IT services. However, the plan was not based on a threat and risk assessment. This increases the chance that the plan may not address significant risks.

The disaster recovery plan had not been updated since it was finalized in April 2008. Since that time there have been changes in PA Parkland. There was a limited test of the plan in 2009. The documentation for the test included recommended actions. PA Parkland did not document action taken on the recommendations. Not having an up-to-date and tested disaster recovery plan increases the risk that systems and data may not be available when needed.

3. We recommend that the Prince Albert Parkland Regional Health Authority maintain an up-to-date and tested disaster recovery plan based on a threat and risk assessment.

Maintain the integrity of systems and data

We expected PA Parkland to have processes for maintaining the integrity of its systems and data by implementing adequate configuration, update, monitoring, and IT operation processes. Adequate processes require approving and testing system changes before implementation. PA Parkland must also ensure that it has adequate processes for running and maintaining its computers.

PA Parkland uses change management processes extensively to manage the work of its service providers. The change management processes are defined and consistent. Before changes are made, the change management process records approvals for implementation, testing, and back-out plans.

We discuss PA Parkland's processes for configuration, updating, and monitoring of its systems and data in more detail in the preceding sections.

Glossary

Account—A unique identity set up on a computer or network that allows access to specific systems and data.

Application—A software program. This includes programs such as word processors, spreadsheets, database programs, accounting programs, etc.

Backup (noun)—A copy of systems or data to be used when the originals are not available (e.g., because of loss or damage).

Change management—An organized approach for introducing changes into a program or process, used to minimize unintended consequences.

Configure—To set up or arrange in order to achieve a specific purpose (e.g., maximize security).

Data centre—A central location for computer network hardware and software, especially storage devices for data.

Disaster recovery plan—A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

Encryption—A method of putting information in code so that only authorized users will be able to see or use the information.

Environmental controls—The controls in place at an organization to manage risks posed by the physical location of computers or network equipment. Examples include fire suppression systems, moisture detectors, and uninterruptable power supplies.

Firewall—Software and/or hardware intended to restrict or block access to a network or computer. Firewalls can be set up to only allow certain types of data through.

IT strategic plan—A plan indicating how an organization intends to use IT to further its business goals and objectives.

Network—A group of computers that communicate with each other.

Physical access controls—The controls in place at an organization that restrict unauthorized people from gaining physical access to computers or network equipment. Examples include locked doors and cabinets, and video surveillance systems.

Server—A computer that hosts systems or data for use by other computers on a network.

USB memory device—A compact memory device that uses a USB (Universal Serial Bus) interface. Also called a flash drive, thumb drive, or memory stick.

User access controls—The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.

Wiring closet—A central location for connecting network cables.

Selected references

Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants. (2009). *Trust services principles, criteria, and illustrations*. New York: Author.

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). *Information technology – Code of practice for information security management*; 2nd Edition. Geneva: Author.

Provincial Auditor Saskatchewan. (2007). Chapter 11F – IT security. In *2007 Report – Volume 3*. Regina: Author.

Provincial Auditor Saskatchewan. (2009). Chapter 10C – Electronic health records. In *2009 Report – Volume 3*. Regina: Author.

Provincial Auditor Saskatchewan. (2010). Chapter 11D - Information technology security. In *2010 Report – Volume 2*. Regina: Author.

IT Governance Institute. (2007). *CobiT4.0*. Rolling Meadows, IL: Author.

This page left blank intentionally.