Equipment disposal

10D

Main points

Agencies have a duty to ensure that sensitive information is secure. One area of risk is when agencies dispose of information technology and communications equipment (such as computers, faxes, and photocopiers) that contain sensitive information.

We examined whether Heartland Regional Health Authority (Heartland) had adequate controls to secure electronic information during disposal of information technology and communications equipment for the six month period ending August 31, 2009. We found Heartland had adequate controls, except it needs to:

- document the procedures it uses to remove confidential information during disposal of information technology and communications equipment
- maintain a current list of capital assets
- document that it follows its approved policy and procedures when disposing of information technology and communications equipment
- regularly verify that its procedures for disposal of information technology and communications equipment are effective

We recommend that public agencies consider their processes to ensure that the equipment they dispose of does not contain sensitive information.

Introduction

This chapter provides the results of our audit of Heartland Regional Health Authority's (Heartland's) controls to secure electronic information during disposal of information technology and communications equipment.

The Regional Health Services Act makes regional health authorities responsible for the planning, organization, delivery, and evaluation of health services in their health regions. Heartland provides health care services to a population of approximately 44,000 people over an area of approximately 41,000 square kilometres in west-central Saskatchewan.[1]

To carry out its role, Heartland must manage health care information. Heartland has a duty to protect personal health information (including confidentiality and destruction) as described in *The Health Information Protection Act*. One area of risk involves disposal of equipment that contains health information, including personal health information.

Ensuring security of health care information upon disposal of equipment is of particular importance to patients and regional health authorities. Unauthorized persons could access information if it is not properly erased from information technology or communications equipment prior to disposal.

Securing personal health information during disposal of equipment is vital to protecting the interests of patients. Inadequate controls could result in unauthorized disclosure of sensitive health information, breach of the statutory duty to safeguard information, harm to the affected individuals, and loss of public confidence for a regional health authority.

Audit objective, criteria, and conclusion

The objective of this audit was to assess whether Heartland had adequate controls to secure electronic information during disposal of information technology and communications equipment for the six-month period ending August 31, 2009. We did not examine controls related to

[1] http://www.hrha.sk.ca/ (August 13, 2009)

disposal of clinical equipment (i.e., equipment used for diagnosis and treatment).

To conduct this audit, we followed the *Standards for Assurance Engagements* established by The Canadian Institute of Chartered Accountants. To evaluate Heartland's controls, we used criteria based on the work of other auditors and current literature listed in the selected references. Heartland agreed with the criteria (see Exhibit 1).

Exhibit 1—Audit criteria

To have adequate controls to secure electronic information during disposal of information technology and communications equipment, we expected Heartland to:

1. Set policies and procedures for disposal of equipment storing electronic information
2. Identify relevant equipment prior to disposal
3. Ensure sensitive data is removed or securely overwritten prior to disposal

We concluded that, for the six month period ending August 31, 2009, Heartland Regional Health Authority's controls to secure electronic information during disposal of information technology and communications equipment were adequate except that it needs to:

- **document its procedures to remove confidential information during disposal of information technology and communications equipment**
- **maintain a current list of capital assets**
- **document that it follows its approved policy and procedures when disposing of information technology and communications equipment**
- **regularly verify that its procedures for disposal of information technology and communications equipment are effective**

In the next section, we set out key findings and recommendations related to the criteria. Our expectations are set out in italics under each subheading.

Key findings and recommendations

Set policies and procedures

We expected Heartland to assign responsibility for handling the disposal of equipment and communicate this to all staff. The policy and procedures should specify what types of equipment are included under the policy and a desired end-state for the equipment. The policy and procedures should also specify disposal methods for different types of equipment. Also, Heartland should regularly review and update its policy and procedures.

Heartland has developed a policy and procedures for the disposal of equipment. The policy and procedures apply to specified "information technology hardware assets" (IT equipment) which includes computers, telecommunications equipment, photocopiers, and other devices managed by Heartland's Information Technology group. The policy is applicable to all employees and specifically assigns the responsibility for disposal of these assets to the Information Technology group. This group is also responsible for acquisition and maintenance of all such assets.

The policy and procedures developed for the disposal of IT equipment were introduced in May 2009. Heartland has told us that its standard approach is to review and update policies and procedures every second year. Heartland communicated the policy and procedures—including the responsibility for disposal—through its updates of the policy and procedures manual. Copies of this manual are kept at Heartland's facilities located in 16 different communities. Heartland also sent notification emails to staff when the policy and procedures were implemented.

The policy and procedures specify a desired end-state for IT equipment. The policy requires that confidential information remaining on the hardware be destroyed to make the data unrecoverable.

The Information Technology group uses several methods to remove information from IT equipment. These methods are not specified in Heartland's policy and procedures, but have been selected by the Information Technology group.

There are risks related to relying on undocumented methods. The methods available for the different types of equipment can vary in their efficiency and effectiveness. If a method is ineffective, unauthorized individuals could access confidential information. Another risk would be that changing technology and options make choosing the appropriate destruction method difficult. As well, undocumented methods can result in inconsistency in application among employees. Turnover of key staff can result in lost knowledge regarding the detailed settings for tools used and processes for verification that data is unrecoverable.

1. We recommend that Heartland Regional Health Authority document its procedures to remove confidential information during disposal of information technology and communications equipment.

Identify relevant equipment prior to disposal

We expected Heartland to identify the specific equipment that falls under the disposal of equipment policy and keep information regarding identified equipment current. Procedures for disposal should also link to Heartland's capital asset management procedures.

The Information Technology group is responsible for acquisition, maintenance, and disposal of IT equipment. The group maintains a list of IT equipment in service. IT equipment is identified by location, model, and other information such as employees assigned to the equipment. Updates of this information occur when there are service requests. Heartland developed the list in 2008 and management informed us that Heartland plans to do a full review of the list in the current year for updates and completeness. However, Heartland does not have a formal review and update process.

There are over 100 IT equipment items, costing more than $600,000 that Heartland treats as capital assets. Given that there have been no capital asset counts performed in the past five years, this information is outdated. Outdated information increases the risk equipment with sensitive or confidential information will not be disposed of properly.

We have recommended that Heartland Regional Health Authority maintain a current list of capital assets in the Regional Health Authority chapter in this report.

Management has indicated that the Information Technology group plans to develop a new Information Technology asset tagging and numbering process. This process and log will supplement the information already maintained. Management states that this new process will allow the Information Technology group to better track IT equipment.

Ensure sensitive data is removed or securely overwritten prior to disposal

We expected Heartland to securely store IT equipment prior to disposal and follow policies and procedures for all specified equipment. We expected Heartland to verify the effectiveness of its procedures.

The Information Technology group is responsible for disposal of IT equipment. When an asset is identified for disposal, the Information Technology group retrieves the asset from its location and stores the equipment until disposal. This central storage of items allows the Information Technology group to track and control the asset in a secure manner.

Heartland does not document its disposal of IT equipment, for example in a log. Given the potential for sensitive information to remain on IT equipment, it is important to be able to verify that disposal occurred properly and that policies and procedures were followed, including: who disposed of IT equipment, when the equipment was disposed of, and how the equipment was disposed of. It is also important to document reasons for choosing the disposal method if there are alternatives. Due to deficiencies in the asset tracking and documentation process, we were unable to verify that Heartland followed its disposal policy and procedures for all IT equipment.

2. We recommend that Heartland Regional Health Authority document that it follows its approved policy and procedures when disposing of information technology and communications equipment.

As technology changes, procedures for disposal of IT equipment can become less effective. It is important to regularly verify that procedures are effective in removing sensitive data. Heartland has not formally tested its procedures to ensure they are effective.

3. We recommend that Heartland Regional Health Authority regularly verify that its procedures to remove sensitive information from information technology and communications equipment are effective.

Selected references

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

National Institute of Standards and Technology. (2006). *Information security - Recommended security controls for federal information systems.* Gaithersburg, MD: Author.

The University of Auckland - New Zealand. (2007). *Computer and Network Security Management Policy.* (Version 1.4). http://www.security.auckland.ac.nz/ComputerandNetworkSecurityManagementPolicy.htm (28 Oct 2009).