

**SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**



FROM: County Auditor-Controller

SUBMITTAL DATE:
January 12, 2009

SUBJECT: Internal Audit Report 2008-004.2: Riverside County Regional Medical Center, Disposal of Computers and Related Equipment

RECOMMENDED MOTION: Receive and file Internal Audit Report 2008-004.2: Riverside County Regional Medical Center, Disposal of Computers and Related Equipment.

BACKGROUND: The Auditor-Controller completed an audit of the Riverside County Regional Medical Center (RCRMC) to provide the Board of Supervisors and RCRMC management an independent assessment about the adequacy and effectiveness of internal controls over the disposal of desktop and notebook computers, portable media devices, and stored electronic data.

The audit found adequate internal controls were maintained over the disposal process of computers, laptops, mobile devices, as well as the removal of confidential county information. To strengthen internal controls, the return of mobile devices from resigning employees should be documented to support the transfer of the asset back to the department.

Management concurred with the finding and recommendation and provided a corrective action plan. We will follow-up within one year to verify that RCRMC management took the planned corrective action.

Robert E. Byrd

Robert E. Byrd
County Auditor-Controller

FINANCIAL DATA	Current F.Y. Total Cost:	\$ 0	In Current Year Budget:	N/A
	Current F.Y. Net County Cost:	\$ 0	Budget Adjustment:	N/A
	Annual Net County Cost:	\$ 0	For Fiscal Year:	N/A

SOURCE OF FUNDS: N/A	Positions To Be Deleted Per A-30	<input type="checkbox"/>
	Requires 4/5 Vote	<input type="checkbox"/>

C.E.O. RECOMMENDATION:

County Executive Office Signature

Policy
 Policy
 Consent
 Consent
 Dept Recomm.:
 Per Exec. Ofc.:

Prev. Agn. Ref.: | **District:** | **Agenda Number:**

Departmental Concurrence



County of Riverside

INTERNAL AUDIT REPORT

Riverside County Regional Medical Center Disposal of Computers and Related Equipment

November 10, 2008

Office of
Robert E. Byrd, CGFM
County Auditor-Controller

4080 Lemon Street
P.O. Box 1326
Riverside, CA 92502-1326



OFFICE OF THE
COUNTY AUDITOR-CONTROLLER

County Administrative Center
4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
(951) 955-3800
Fax (951) 955-3802



COUNTY OF RIVERSIDE
AUDITOR-CONTROLLER
Robert E. Byrd, CGFM
AUDITOR-CONTROLLER

Bruce Kincaid, MBA
ASSISTANT
AUDITOR-CONTROLLER

November 10, 2008

Douglas D. Bagley
Chief Executive Officer
Riverside County Regional Medical Center
26250 Cactus Avenue
Moreno Valley, CA 92555

Subject: **Internal Audit Report 2008-004.2: Riverside County Regional Medical Center,
Disposal of Computers and Related Equipment**

Dear Mr. Bagley:

We have completed an audit of computers and related equipment disposal procedures for the Riverside County Regional Medical Center as one of three departments selected for detailed testing as part of a countywide audit. We conducted the audit during the period August 8, 2007, through March 31, 2008, for operations of July 1, 2005, thru March 31, 2008.

Our primary objective was to provide an independent assessment about the adequacy of internal controls over the disposal of computers and related equipment, including the removal of stored confidential county information.

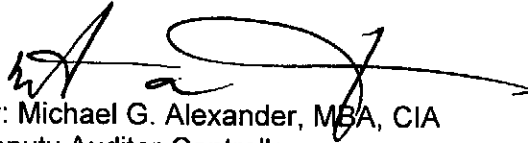
We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain reasonable assurance that our objective as described in the preceding paragraph is achieved. An audit includes examining, on a test basis, evidence about the adequacy and efficiency of internal controls, compliance with applicable laws, reliability of financial information, and performing such other procedures as we considered necessary in the circumstances. We believe the audit provides a reasonable basis for our opinion.

Adequate internal controls were maintained over the disposal process of computers, laptops, mobile devices, as well as the removal of confidential county information. To strengthen internal controls, the return of mobile devices from resigning employees should be documented to support the transfer of the asset back to the department. Throughout the audit, we discussed the results contained in this report with the appropriate levels of management.

A copy of the reply from the RCRMC management is attached to this report, and excerpts from the reply were presented in the appropriate section of the report. Management concurred to implement the recommended corrective action. We will follow-up within one year to verify that management implemented the corrective action.

We thank the Riverside County Regional Medical Center's management and staff for their full cooperation; their assistance contributed significantly to the successful completion of the audit.

Robert E. Byrd, CGFM
Auditor-Controller



By: Michael G. Alexander, MBA, CIA
Deputy Auditor-Controller

cc: Board of Supervisors
County Counsel
Executive Office
Grand Jury

Table of Contents

	Page
Executive Summary	1
Results	3
Management Reply	Appendix

Executive Summary

Audit Objective

Our primary objective is to provide the Board of Supervisors and RCRMC management an independent assessment about the adequacy and effectiveness of internal controls over the disposal of desktop and notebook computers, portable media devices and stored electronic data.

Overview

Private and confidential information like patient healthcare information, among many others, may be stored in computer hard drives and in portable electronic devices such as USB hard drives, flash drives, recordable DVDs, PDAs, and cell phones. The permanent and irreversible removal of data stored on equipment, prior to disposal, is vital to prevent inadvertent unauthorized data disclosure.

RCRMC opted to physically destroy computer hard drives rather than removing data using commercially available demagnetizer machines or data sanitizing software programs. The aim for removing data from hard drives is to permanently erase the data beyond recovery. The physical destruction of hard drives serves the same purpose by making the device unusable and beyond repair. RCRMC believes the latter is the best method.

RCRMC Policy 107.7 (Computer Access and Use) establishes the standards and safeguards for user access to the RCRMC computer system following the guidelines set by Health Insurance Portability and Accountability Act (HIPAA) and Board of Supervisors' Policy A-58 (Enterprise Information Systems Security Policy). Policy 107.7 prohibits RCRMC staff from taking outside of its campuses computers containing patient healthcare information except when needed in providing direct patient healthcare services. Although it is not covered by any of the present policies, RCRMC is directing all employees to refrain from using flash drives.

Audit Methodology

Our audit methodology is aimed at ascertaining whether the process for disposing computers and portable media devices provides reasonable assurance that stored electronic data are properly eliminated, and governing regulations and policies are complied with.

The following are the procedures we performed:

- Gained an understanding of the applicable, codes, regulations, policies and procedures;

- Documented current practices by interviewing personnel, walking through and observing processes;
- Verified whether current practices adhere to governing codes, regulations, and established county policies and procedures by reviewing reports, records, and other evidences;
- Ascertained whether an accounting system is maintained for equipment issued to employees, and equipment are recalled from terminated employees; and
- Evaluated audit findings and evidences to form our professional opinion.

Conclusion

The audit found adequate internal controls were maintained over the disposal process of computers, laptops, mobile devices, as well as the removal of confidential county information. To strengthen internal controls, the return of mobile devices from resigning employees should be documented to support the transfer of the asset back to the department.

The details regarding the audit results, findings and recommendations are contained in the body of this report.

Results

Computers

The RCRMC Information Services (IS) inspects all desktop and notebook computers before they are sent to county surplus for disposal. IS removes the hard drives, memory chips, and other salvageable parts from the computers. The recovered parts are recycled except for the hard drives which are smashed and mutilated with a sledge hammer to render them unusable. The IS management believes that destroying the hard drives in this manner is secure and effective in preventing any access to the stored data. In our judgment, as long as the hard drives are disfigured and mangled beyond repair, the physical destruction of hard drives serves the same purpose as permanently removing the data. For security reasons, it is important that the process is strictly monitored, witnessed, and documented to ensure that all hard drives are collected and permanently destroyed.

Electronic Media Devices

RCRMC staff use electronic media devices including recordable DVDs, PDAs, and cell phones. The IS department approves the purchase of electronic media devices, except USB flash drives as their use are not allowed. Notebook computers are purchased with recordable DVDs.

The assignment of PDAs and cell phones is determined based upon staff's need and approved by an official designated to review and authorize computer equipment acquisitions. The Communications department maintains a record of PDAs and cell phones and their assigned custodians.

We tested whether terminated employees returned portable electronic devices issued to them. To accomplish this, we reviewed the PDAs and cell phones due from employees, who had resigned during the period June through December, 2007. Our test found the documentations on file to evidence the return of PDAs and cell phones due from the employees are in order.

Finding 1

There is no formal document establishing responsibility for collecting portable electronic devices due from resigning employees. The Information Services, Communications, and Administration departments share this responsibility. The lack of a documented procedure increases the likelihood that portable electronic devices due from resigning employees may not be retrieved. The Auditor-Controller

Standard Practice Manual 104 requires departments maintain an effective system of internal control that includes safeguarding of assets.

Recommendation 1 Develop procedures that ensure all portable media devices due from resigning employees are returned.

Management Reply "Concur. RCRMC concurs with the recommendation. Reviewed with Human Resources. We have discussed possible solutions.

Actual/estimated Date of Corrective Action: November-December, 2008

The current proposed solution:

Create a database of employee supplied mobile devices. HR will check the database using a "user friendly" form or interface to see if the employee has equipment issued to them. HR will request equipment returns. Information Services and Communications will keep the information "up to date."

Policy, Procedures, Processes, and applications need to be built and implemented. Training will be needed.

PDA's currently being kept for issuance in Administration will be turned into Information Services to keep track of."



Memorandum

Date: June 16, 2008
To: Auditor-Controller
Audits and Specialized Accounting Division
From: Douglas Bagley, Chief Executive Officer *DB*
Subject: Reply to Draft Audit Report - Countywide Disposal of Computer and Related Equipment Audit

Recommendation Number 1:

Develop a policy and process that ensures mobile devices are returned by employees prior to the termination of employment.

a. **Management position concerning the recommendation:**

XX Concur _____ Disagree

b. **Comments:**

RCRMC concurs with the recommendation. Reviewed with Human Resources. We have discussed possible solutions.

c. **Actual/estimated Date of Corrective Action: November – December, 2008**

The current proposed solution:

Create a database of employee supplied mobile devices. HR will check the database using a "user friendly" form or interface to see if the employee has had equipment issued to them. HR will request equipment returns. Information Services and Communications will keep the information "up to date".

Policy, Procedures, Processes, and applications need to be built and implemented. Training will be needed.

PDA's currently being kept for issuance in Administration will be turned into Information Services to keep track off.

d. **Estimated cost to implement recommendation (If material)**

Capital costs should be \$0.

Total Labor costs should be 500 hours or less (Includes HR, Applications, Communications, Policy writing, Procedures, Training, etc.)