



**CITY OF COLORADO SPRINGS
OFFICE OF THE CITY AUDITOR**

**09-12 – MEMORIAL HEALTH SYSTEM
NORTH DATA CENTER REVIEW**

PUBLIC REPORT

June 18, 2009

Jeff Litchfield
City Auditor

Denny Nester, CPA CIA CGFM CFE
Assistant City Auditor

Roy Florey, CIA, CISA
Principal Auditor





City of Colorado Springs



Colorado Springs Utilities
It's how we're all connected



Memorial Health System



Office of the City Auditor

Public Report

Date: June 18, 2009

To: Honorable Mayor and Members of City Council
Members of the Memorial Health System Board of Trustees
Members of the Memorial Health System Audit Committee

Re: 09-12 - Memorial Health System North Data Center Review

We conducted an audit of the internal security controls for Memorial Health System's North Data Center.

The purpose of this audit was to review the North Data Center's security, policies, and procedures to ensure the confidentiality, integrity, and availability of the data center and the hardware stored in the data center.

We found the North Data Center's security, policies, and procedures were sufficient to provide reasonable protection over the confidentiality, integrity, and availability of the data center and the hardware stored in the data center. However, during the course of our audit, we did identify areas where we believe internal controls can be strengthened. These areas are listed on the pages that follow.

As always, feel free to contact me if you have any questions.

Sincerely,

Jeff Litchfield
City Auditor

Cc: Dr. Larry McEvoy II, Chief Executive Officer
Tom Kerwin, Chief Information Officer
Bob Barrett, Director of Information Technology
Mike Scialdone, Chief Financial Officer
Joe Taylor, Director Facilities Management
John Wyckoff, Compliance Officer

CITY AUDITOR JEFF LITCHFIELD, CPA CIA CFE CGAP

TEL 719-385-5991 • FAX 719-385-5699 • HOTLINE 719-385-2387 • REPORT WEBSITE WWW.CITYAUDITOR.ORG
30 South Nevada Avenue, Suite 604 • P.O. Box 1575, Mail Code 640 • Colorado Springs, CO 80901-1575

Table of Contents

09-12 – MEMORIAL HEALTH SYSTEM NORTH DATA CENTER REVIEW

PUBLIC REPORT

	Page
Introduction	
Authorization	2
Organizational Placement	2
Scope and Methodology	2
Background	3
Overall Opinion	3
Findings, Recommendations, and Responses	
1. The Data Center sign-in sheet was not consistently completed and was missing a required field	4
2. The Data Center Emergency Power Off switches had not been tested since they where initially installed	5
3. The Data Center did not have a water removal system	6

Abbreviations and Acronyms used in this Report

EPO	Emergency Power Off
IS	Information Services

Introduction

AUTHORIZATION

We conducted an audit of Memorial Health System's (Memorial) North Data Center (Data Center). We conducted this audit under the authority of Chapter 1, Article 2, Part 7 of the Colorado Springs City Code, and more specifically parts 703 and 705, which state:

1.2.703: ENSURE PUBLIC ACCOUNTABILITY:

The City Auditor shall ensure that administrative officials are held publicly accountable for their use of public funds and the other resources at their disposal. The City Auditor shall investigate whether or not laws are being administered in the public interest, determine if there have been abuses of discretion, arbitrary actions or errors of judgment, and shall encourage diligence on the part of administrative officials.

1.2.705: DETERMINE EFFECTIVENESS AND EFFICIENCY OF PROGRAMS:

The City Auditor shall determine the extent to which legislative policies are being efficiently and effectively implemented by administrative officials. The City Auditor shall determine whether City programs are achieving desired objectives. The City Auditor shall review the administrative control systems established by the enterprises, department or group managers and by the City Manager, Utilities Executive Director and Memorial Hospital Executive Director and determine whether these control systems are adequate and effective in accomplishing their objectives.

ORGANIZATIONAL PLACEMENT

The Office of the City Auditor is structured in a manner to provide organizational independence from the entities it audits. This independence is accomplished by the City Auditor being appointed by and reporting directly to the City Council. The audited entity in this audit was Memorial Health System, which is an enterprise of the City of Colorado Springs under the direction of its Chief Executive Officer. The Chief Executive Officer reports to the Memorial Health System Board of Trustees, who are appointed by the City Council.

SCOPE AND METHODOLOGY

The purpose of this audit was to review the North Data Center's security, policies, and procedures to ensure the confidentiality, integrity, and availability of the Data Center and the hardware stored in the Data Center.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*, a part of the Professional Practices Framework promulgated by the Institute of Internal Auditors. The audit included such test of records and other supporting documentation as was deemed necessary in the circumstances. We reviewed the internal control structure and performed compliance tests. Sufficient competent evidential matter was gathered to support our conclusions.

Introduction

BACKGROUND

Memorial North Hospital was opened in 2007. The Data Center is located in the basement of the Memorial North Hospital and is unmanned. The Information Services (IS) Department has an office area adjacent to the Data Center, but no one has a desk/office within the Data Center. The Alarm Dispatch Center is responsible for monitoring cameras and environmental sensors associated with the Data Center. The Facilities Department provides maintenance for the Data Center along with contracted 3rd parties who test various systems within the Data Center.

OVERALL OPINION

We found the North Data Center's security, policies, and procedures were sufficient to provide reasonable protection over the confidentiality, integrity, and availability of the Data Center and the hardware stored in the Data Center. However, during the course of our audit, we identified areas where we believe internal controls can be strengthened. These areas are listed on the pages that follow.

***We have made no determination as to which findings are more important than others.
Therefore, the findings are not listed in order of importance.***

Findings, Recommendations, and Responses

1. The Data Center sign-in sheet was not consistently completed and was missing a required field.

The Data Center Standards indicated that the Data Center sign-in sheet should have a field for the Memorial employee to sign indicating they escorted the visitor while in the Data Center. The sign-in sheet reviewed did not have a field for the Memorial employee to print their name or sign indicating they escorted the visitor while in the Data Center. The sheet also showed inconsistencies when visitors signed in. Several visitors did not document the time they left the Data Center while others did not provide a signature when signing in.

Sign-in sheets could be used to determine when a visitor entered the Data Center and their name. A sign-in sheet with inaccurate data makes it difficult to determine all the details of a visitor who entered the Data Center. If an incident occurred at a specific time in the Data Center and the visitor sign-in sheet did not accurately show time in and out, it could be difficult to determine if a specific visitor is responsible. However, as a compensating control, Memorial had implemented cameras that cover the interior of the Data Center and the Data Center entrances. The cameras would record the visitor and Memorial employee entering the Data Center. An accurate sign-in sheet would help with an investigation by providing a time frame for when a visitor was in the Data Center limiting how much camera footage needed to be reviewed.

Auditor's Recommendation:

Memorial should add a field for the Memorial employee's name and signature indicating they escorted the visitor while in the Data Center. Memorial employees should ensure the visitor accurately fills out all fields on the sign-in sheet.

Memorial's Response:

We agree with this finding. The sign-in sheet was modified to include the name of the Memorial Health System employee that escorts any visitor into the Data Center. Training was provided to ensure accuracy and completeness of the form.

Findings, Recommendations, and Responses

2. The Data Center Emergency Power Off (EPO) switches had not been tested since they were initially installed.

EPOs are designed to shut off all power to the area the EPO controls in case of emergency, such as the Data Center. The EPOs in the Data Center were tested after they were initially installed in 2007. Since that time, they had not been tested to make sure they are functioning properly.

Routine maintenance and testing could detect faulty wiring or malfunctioning EPOs and help ensure they would function properly in case of an emergency. Without testing and maintenance, there is the possibility that the EPO will not function properly causing additional damage or injury.

Auditor's Recommendation:

Memorial should provide develop a periodic testing and maintenance schedule for the EPOs in the Data Center to ensure they are functioning properly.

Memorial's Response:

We agree with the finding and agree in part with the recommendation. Full-functioning live EPO testing would require that all systems in the Data Center be suddenly turned off without the opportunity for a graceful shutdown. This would certainly cause planned downtime for systems that assist in providing high quality healthcare. In addition, the sudden shutdown of systems can cause unpredictable results when power is restored. This can cause unplanned downtime events for a healthcare system. The Information Services Department will work with our UPS maintenance vendor to determine if there is any practical alternative to a live EPO test

Findings, Recommendations, and Responses

3. The Data Center did not have a water removal system.

The Data Center had an increased water threat since it was in the basement and there were water pipes in the ceiling. If a pipe burst or leaked, there would have been notification since there was a water infiltration sensor in the floor. However, there would have been no automated way to remove the water. Water could then come in contact with electrical wiring and network cabling running under the floor and potentially damage equipment in the Data Center.

Auditor's Recommendation:

Memorial should install an automated water removal system in the Data Center. The system should also be on a preventative maintenance schedule to ensure it is working properly.

Memorial's Response:

We agree with this finding. There is some risk associated with water leaking into the Data Center because of its location in the basement. We disagree with the recommendation. The cost of an automated water removal system is disproportionate to the probability of the necessity to remove large quantities of water. The existing water infiltration system will notify the alarm dispatch center as soon as water is detected. Memorial Health System believes that the water sensing system provides the alerting necessary to respond to water threats before large quantities of water require automated removal. The Information Services Department shall work with the Facilities Management Department to ensure there are policies and procedures in place to respond to water threats in the Data Center.