



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

**10-11 MEMORIAL HEALTH SYSTEM E-CLIPS
INITIAL SYSTEM REVIEW**

PUBLIC REPORT

MAY 12, 2010

Denny Nester, CPA CIA CGFM CFE
Interim City Auditor

Roy Florey, CIA, CISA
Principal Auditor





Office of the City Auditor

Public Report

Date: May 12, 2010

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: 10-11 Memorial Health System E-CLIPS Initial System Review Audit

We conducted an audit of the internal security controls for Memorial Health System's (Memorial) E-CLIPS system. The E-CLIPS system is the primary electronic medical record documentation system utilized by Memorial.

The purpose of this audit was to review the E-CLIPS system to ensure adequate controls have been implemented to protect patient records. The audit focused on three aspects of E-CLIPS including the application, database, and server. Internal controls were reviewed to ensure each aspect was providing adequate security and data integrity.

We conclude that overall, the existing policies and procedures and internal control measures are adequate. However, during the course of our audit, we identified four areas where we believe internal controls could be strengthened. They are listed in the attached report.

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

Sincerely,

A handwritten signature in black ink, appearing to read "Denny Nester".

Denny Nester
Interim City Auditor

Cc: Dr. Larry McEvoy II, Chief Executive Officer
Mike Scialdone, Chief Financial Officer
Jonathan Valez, Interim Chief Information Officer
Bob Barrett, Director of Information Technology
Marilyn Goodloe, Director of Information Systems
John Wyckoff, Compliance Officer

INTERIM CITY AUDITOR DENNY NESTER, MBA CPA CIA CGFM CFE CGAP

TEL 719-385-5991 • FAX 719-385-5699 • FRAUD HOTLINE 719-385-2387 • REPORT WEBSITE WWW.CITYAUDITOR.ORG
107 North Nevada Avenue, Suite 200 • P.O. Box 1575, Mail Code 1542 • Colorado Springs, CO 80901-1575


Table of Contents

10-11– MEMORIAL HEALTH SYSTEM E-CLIPS INITIAL SYSTEM REVIEW

PUBLIC REPORT

	Page
Introduction	
Authorization	2
Organizational Placement	2
Scope and Methodology	2
Background	3
Overall Opinion	3
Findings, Recommendations, and Responses	
1. Generic administrative userids were utilized	4
2. Password policies needed to be strengthened, enforced, and consistent	5
3. User access was not adequately reviewed and maintained.	6
4. The change control policy was inadequate	7

Abbreviations and Acronyms used in this Report



DBA	Database Administrator
IS	Information Systems
SSH	Secure shell

Introduction

AUTHORIZATION

We conducted an audit of Memorial Health System's (Memorial) E-CLIPS system. 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, 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 Board of Trustees, who are appointed by the City Council.

SCOPE AND METHODOLOGY

The purpose of this audit was to review the E-CLIPS system to ensure adequate controls have been implemented to protect patient records. The audit focused on three aspects of the E-CLIPS system including the application, database, and server. Internal controls were reviewed to ensure each aspect was providing adequate security and data integrity.

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 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

E-CLIPS went live in April 2006, and served as the primary electronic medical record documentation system utilized by Memorial. [REDACTED], the main component of E-CLIPS, was installed on [REDACTED] operating system and utilized [REDACTED] database for data storage. Memorial implemented various failover technologies in the event of a failure by one of the systems involved. This helped ensure the availability of the data stored in E-CLIPS.

OVERALL OPINION

Overall, we found adequate controls were implemented to protect patient records and that adequate security and data integrity was provided for the application, database, and server aspects of the E-CLIPS system. However, during the course of our audit, we did identify areas where we believe internal controls could 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. Generic administrative userids were utilized.

The [REDACTED] Administrators (DBA) and the [REDACTED] backup system administrators used generic userids for administration of the systems. When a backup system administrator needed to use the generic userid, they had to access a [REDACTED] database that had the password for this account. When the backup system administrator accessed the [REDACTED] database, an email was sent to the system administrator and IS management indicating the backup system administrator had the password. After the backup system administrator was done using the generic userid, the system administrator changed the password and entered the new password into the [REDACTED] database. While this procedure limited the risk, there was still the risk that both backup system administrators could have the generic userid password. This scenario would make it difficult to determine which backup system administrator logged in since both had the password.

Generic userids could make it difficult to identify who used the userid and what was done during an investigation that relied on logging of the userid. Having more than one individual who can login with the same userid could make logs insufficient since it cannot be determined, through the logs, who used the userid. If a change, malicious or not, was made to the [REDACTED] environment using a generic userid, the logs would not be able to identify the individual who used the generic userid since more than one person could have the password.

Auditor's Recommendation:

We recommend that Memorial provide each administrative user a unique userid with which to login. This process would make it easier to track each user since each would have their own userid.

Memorial's Response:

We agree with the recommendation. All personnel who are responsible for day-to-day administration tasks now have unique userids and passwords for both [REDACTED] and [REDACTED] systems. Any changes made by these users are now more accurately tracked. The generic userids [REDACTED] are still active as they are required by the [REDACTED] operating system and [REDACTED] software respectively. However, the generic userids [REDACTED] can only be used on site (they cannot be used remotely).

Findings, Recommendations, and Responses

2. Password policies needed to be strengthened, enforced, and consistent.

Complex passwords should be utilized to reduce the risk of an attacker guessing passwords. A strict password policy should be used to enforce the practice of users creating complex passwords that are not easily guessed. Consistent policies should be applied to the operating systems, databases, and applications.

Memorial had not implemented password policies for the [REDACTED] operating system or the [REDACTED] database. [REDACTED], Memorial had implemented the following password policy: a minimum password length of [REDACTED] characters, required [REDACTED], and failed login attempts until lockout was set at [REDACTED]. The [REDACTED] password policy did not have passwords expire. The Memorial written password policies required passwords to be [REDACTED] characters long with passwords expiring after [REDACTED].

A lack of strict password policy enforcement could lead to users creating weak passwords that could easily be compromised. A password compromise could lead to the disclosure of sensitive data since the attacker would have access to data the compromised user could access. With longer passwords, the probability of guessing the password would be reduced. For example, a [REDACTED] password that used upper- and lower-case letters, numbers, and punctuation would have [REDACTED] possible combinations. A password of [REDACTED] characters increases the number of combinations to [REDACTED]. By implementing an account lockout threshold of [REDACTED], the risk of guessing a password would be reduced since the account would be locked after the lockout threshold was met.

Auditor's Recommendation:

We recommend Memorial implement strengthened password policies for [REDACTED], [REDACTED], and [REDACTED] that are consistent with written policies. Additionally, Memorial should consider modifying written policies to require passwords be a minimum of [REDACTED] characters long and expire every [REDACTED] days. The policy should also require accounts be locked after [REDACTED] failed logon attempts.

Memorial's Response:

We agree with the recommendation. Memorial Health System will review present password policies and ensure that passwords are at least [REDACTED] characters long and expire [REDACTED]. We will also ensure that accounts are automatically locked out after [REDACTED] attempts. With present processes and tools, the recommended changes would be extremely disruptive to clinical workflow. Because of this, the new policies shall be promulgated only after tools have been identified and implemented which allow for a seamless transition so as to eliminate or lessen the impact to patient care. We expect this to be completed by [REDACTED].

Findings, Recommendations, and Responses

3. User access was not adequately reviewed and maintained.

Memorial did not have formal policies in place that addressed removing or disabling former employees' access to [REDACTED]. Memorial had not been performing scheduled reviews of userids. The reviews could have been used to ensure only valid accounts were enabled and only valid accounts had administrative privileges. Memorial only performed reviews on an as needed basis or if asked to perform the review. Human Resources sent Information Systems (IS) staff notifications of employees no longer working for Memorial. A review of 33 former employees showed that 28 (85%) had an active [REDACTED] userid. A review of [REDACTED] and [REDACTED] groups showed the groups had userids that did not require the privileges they had. Memorial has already addressed the [REDACTED] groups and removed unnecessary userids from the groups.

Active userids for former employees could allow unauthorized access to sensitive information. If a former employee gained access to a computer that is logged onto the network, they would then be able to login to [REDACTED] and access sensitive information. Formal policies and reviews could have detected these accounts giving IS staff the ability to disable access.

Auditor's Recommendation:

We recommend Memorial implement formal policies and procedures that address removing former employees' access to all applications. The policy should include timeframes for removing access and also address implementing formal userid reviews. Memorial should also schedule userid reviews at least annually to ensure only valid userids are enabled, users only have one userid (unless there is a valid reason for multiple userids), and only authorized users have administrative privileges.

Memorial's Response:

We agree with this recommendation. Memorial has updated the formal policy by including in the "Workforce Security Plan and HIPAA Policy Compliance Document" the process for removing former employees' access to all applications (currently a draft document). The policy process flow will state that HR will submit an electronic or voice notification to the IS Security team requesting both the removal of employee access and the timing of such removal. The IS Security team will disable all employee access per the request timing. In order to ensure that all employee access has been removed, a report will be provided identifying any orphaned (non-Memorial provisioned access) accounts. A monthly report listing employees who have accounts will be generated and validated for any discrepancies based on required access. For example, the report would identify if there are users with more than one userid. We expect the policy and procedures to be implemented by [REDACTED]

Findings, Recommendations, and Responses

4. The change control policy was inadequate.

The change control policy did not have a timeframe for IS management approval of the change request and the policy did not indicate how long the requests should be kept on file. Change requests could be system or application changes that need to be made.

Without specified timeframes, change requests may not be processed in a timely manner. Timeframes ensure that IS management approve requests and ensure timely changes are made. Without a timeframe for how long change requests should be kept, change requests could be purged, making it difficult to keep track of changes made along with the timing of the changes.

Auditor's Recommendation:

We recommend the change control policy be updated to include a timeframe for manager approval of change requests and include a timeframe for how long change requests should be kept on file.

Memorial's Response:

We agree with this recommendation. The following additions will be implemented in the Information Services Change Control Policy:

Change Control Requests requiring approval are to be approved within these specified time frames:

Immediate within 24 hours

Urgent within 2 business days

Routine within 15 business days.

Completed change control requests are to be closed within 7 days of the implementation of the change.

Completed change control requests will be kept on file in the active change control database for 30 days after the implementation date. The change control request will be moved to the archive database after 30 days.

Once approved, modifications will be made to the change control application to implement the additions as noted above. This will be completed by June 1, 2010.