

AUDITOR'S REPORT

HARRIS HEALTH SYSTEM EPIC FINANCIAL MODULES ACCESS CONTROLS THREE MONTHS ENDED MARCH 31, 2014



December 4, 2014

**Barbara J. Schott, C.P.A.
Harris County Auditor**

Mike Post, C.P.A.
Chief Assistant County Auditor
Accounting Division

Mark Ledman, C.P.A., M.P.A.
Chief Assistant County Auditor
Audit Division



1001 Preston, Suite 800
Houston, Texas 77002-1817
(713) 755-6505

FAX (713) 755-8932
Help Line (713) 755-HELP

BARBARA J. SCHOTT, C.P.A.
HARRIS COUNTY AUDITOR

December 4, 2014

Mr. George Masi
President and Chief Executive Officer
Harris Health System
2525 Holly Hall
Houston, Texas 77054

RE: Harris Health System Epic Financial Modules Access Controls for the three months ended March 31, 2014

The Audit Services Department performed procedures relative to the Harris Health System (Harris Health) Epic Financial Modules Access Controls. The objective of the engagement was to evaluate critical controls for providing the appropriate level of user access to Epic financial modules, changing user access when necessary, and terminating user access that is no longer required. The following procedures were performed:

- Reviewed written policies and procedures for granting, monitoring, and terminating user access.
- Reviewed and selectively evaluated current Epic financial module user role security templates and user assignments.
- Reviewed and selectively tested controls for:
 - Changing user security role templates.
 - Providing new or changing existing user access.
 - Timely terminating user access no longer required.
- Determined whether information technology has policies and procedures for accessing Epic remotely or through mobile devices.

The engagement process included providing former President and Chief Executive Officer, Mr. David Lopez, with engagement and scope letters and conducting an entrance and exit conference with Harris Health personnel. The purpose of the letters and conferences were to explain the process, identify areas of concern, describe the procedures to be performed, discuss issues identified during the engagement, and solicit suggestions for resolving the issues. A draft report was provided to you and your personnel for review.

The enclosed Auditor's Report presents the significant issues identified during our procedures, recommendations developed in conjunction with your staff, and any actions you have taken to

Mr. George Masi
President and Chief Executive Officer

implement the recommendations. Less significant issues and recommendations have been verbally communicated to your staff.

We appreciate the time and attention provided by you and your staff during this engagement.

Sincerely,



Barbara J. Schott
County Auditor

cc: Harris Health System Board of Managers
District Judges
County Judge Ed Emmett
Commissioners:
 R. Jack Cagle
 El Franco Lee
 Jack Morman
 Steve Radack
Devon Anderson
Vince Ryan
William J. Jackson

TABLE OF CONTENTS

OVERVIEW	5
RESULTS	7
ISSUES AND RECOMMENDATIONS	8
Assigning User Templates	8
Changing Epic User Security Settings.....	8
Terminating Contractors Access	9
Verifying Current Access	10
RISK ASSESSMENT AND SUMMARY OF RECOMMENDATIONS.....	11

OVERVIEW

Harris Health employees use software acquired from Epic (Epic financial modules) to perform tasks that include recording and/or accumulating patient charges, generating bills for services, recording payments for services, and maintaining patient billing records. Harris Health Policy 3.11.807, *Information Access Management Policy* restricts access provided to information systems users (employees and contractors) to the minimum required to perform their job responsibilities.

Standard user access templates were developed that correspond to different user requirements for access so management in the work areas that access the Epic financial modules (user departments) can provide employees and contractors the appropriate level of user access. The templates were developed through a collaborative process that included the user departments, and the Corporate Compliance (Corporate Compliance) and Information Technology (IT) Departments.

Management in the user departments and Corporate Compliance identified the access that was needed for the users to perform job duties in their areas. A review was also performed for separation of duties to ensure users would not be able to perform incompatible activities in Epic. IT developed standard templates that were tested and assigned to users based on user needs identified.

There is also a process for establishing new or changing existing templates. Management in departments requiring new templates or revisions to existing templates must submit a request to the IT Department's help desk. Employees in IT forward the request to Corporate Compliance Management for review and approval, and will only proceed with establishing or changing templates if approval is received. Creating new templates or changing existing templates is also controlled through the IT Change Control process to ensure required testing is performed and approvals are received and documented before changes are implemented.

Assigning new users to an existing template or changing current users to a different existing template (because of a change in job duties) does not require the approval of Corporate Compliance Management. However, management in the departments still must submit an IT help desk request. Employees at the IT help desk ensure that the requests are properly approved by the requesting department's management, and that any other needed approvals are received before assigning the access.

Epic financial module access for employees that leave Harris Health ends when the employee's termination is recorded in the PeopleSoft Human Resources system by the employee's manager. Epic financial module access for contractors will end when the departments that authorized the access notify IT that the access is no longer needed.

Twice a year, IT Management sends management in user departments reports that show user access to the Epic financial modules authorized by the departments. IT Management requests that management review the reports, communicate any necessary changes to IT, and affirm in writing that the reports were reviewed and necessary changes were communicated.

IT and the Information Security Department of Corporate Compliance share responsibility for ensuring adequate controls for accessing Epic remotely or through mobile devices. Policies and procedures have been developed and implemented which restrict access to only approved devices and methods for employees and contractors. There are also application and monitoring controls to prevent and/or identify inappropriate access.

RESULTS

Developing and implementing standard user access templates has improved controls for providing access to users of the Epic financial modules. Based on our procedures:

- Current Epic financial module user role security templates and user assignments appear appropriate.
- Controls for the development of new templates and changing existing templates appear adequate.

In addition, the IT and the Information Security Departments have developed and implemented policies and procedures for accessing Epic remotely and/or through mobile devices.

Although controls are adequate, some opportunities for improvements were identified as follows:

- A target date for completing assigning templates to all users of the Epic financial modules should be established.
- Procedures identifying IT employee groups authorized to change user security settings should be documented and distributed to all IT employees, and compliance with procedures monitored using Epic Change Logs.
- Controls for timely terminating user access no longer required should be improved by:
 - Assigning Epic access expiration dates to contractor's that correspond to the length of time the contractors' services will be required.
 - Including users not assigned to templates and IT employee users on reports sent to management for review and to communicate necessary changes in access.

These issues are discussed in more detail in the following Issues and Recommendations matrix.

ISSUES AND RECOMMENDATIONS

Subject	Background	Issue	Recommendation	Management Response
Assigning User Templates	<p>Corporate Compliance Management has provided the leadership in developing and implementing templates for the Epic financial modules.</p> <p>Policy 3.11.807, <i>Information Access Management Policy</i>, restricts access provided to information systems users to the minimum required to perform their job responsibilities.</p>	<p>As of May 2014, approximately 123 of 1,644 (7.5%) active Epic financial module users had not been assigned to templates. As a result, there is a risk that some of the 123 users have more access than needed to perform their job responsibilities, which does not comply with policy, may allow inappropriate access, and may not provide for adequate separation of duties.</p>	<p>Corporate Compliance Management should continue to provide leadership for developing and implementing templates, and should establish a target date for completing the assignment of templates to the 123 remaining users.</p>	<p>We agree with this recommendation and I.T. Management is working with Corporate Compliance to review the list of 123 users that do not have templates and identify the appropriate corporate compliance approved template that should be assigned to these users.</p> <p>The targeted completion date for assigning a template for each of the users is by 12/31/14</p>
Changing Epic User Security Settings	<p>IT's informal procedures prohibit IT employees with the ability to change their own Epic user security settings from making such changes without management approval. Reports from Epic (Epic Change Logs) are available and can be reviewed to identify user security</p>	<p>An IT employee from an area that should not be allowed to change Epic user security settings made changes to their own security settings. The changes were identified through a review of a sample of five Epic user security settings changes that occurred during the</p>	<p>IT Management should modify their official document, <i>Epic Privileged User Role-Based Access Standards</i>, to clearly define the IT employee groups that are and are not authorized to make changes to Epic security settings. The updated <i>Standards</i> should be signed by the Chief</p>	<p>We agree with this recommendation.</p> <p>The Epic Privileged User Role-Based Access Standards document will be updated and approved by the C.I.O. by 9/29/14.</p> <p>The change in question was reviewed with the auditors and deemed part of a go live</p>

ISSUES AND RECOMMENDATIONS

Subject	Background	Issue	Recommendation	Management Response
(Continued) Changing Epic User Security Settings	settings and other changes made.	<p>three months ended March 31, 2014. IT Management informed Audit Services that the changes were investigated and correlated to work being performed by the employee during the period.</p> <p>In addition, IT Management informed us the employee was counseled after Audit Services brought the changes to their attention.</p> <p>Changes to Epic user security setting by IT employees not authorized to make the changes increases the risk of inappropriate changes, or of changes occurring that could adversely impact computer operations.</p>	<p>Information Officer and distributed to all IT employees.</p> <p>In addition, IT Management should periodically review the Epic Change Logs to determine whether user security settings are changed by employees from a group not authorized to make changes. If such changes are identified, appropriate disciplinary action should be taken.</p>	<p>and large change control with this particular item not being documented appropriately. Management will work with employees to insure that all parts of a go live change are documented in the appropriate change control.</p>
Terminating Contractors Access	Management in user departments must notify IT to disable access to Epic financial modules provided to contractors that is no	Contractors' can continue to access the Epic financial modules after their work at Harris Health is completed if management in the	IT Management should implement a process of assigning access to contractors with expiration dates that correspond to the	We agree with this recommendation. The Help Desk has a policy where they create active directory accounts for contractors, if

ISSUES AND RECOMMENDATIONS

Subject	Background	Issue	Recommendation	Management Response
(Continued) Terminating Contractors Access	longer needed. The access of any users that do not access the Epic financial modules for a period of 180 days will be disabled by IT employees that monitor access.	department that authorized the access does not notify IT to disable it. As a result, there is an increased risk that contractors no longer performing work for Harris Health will be able to inappropriately access the Epic financial modules.	anticipated length of time the outside contractors' services are expected to be required.	the contractor is here for less than 90 days, the help desk puts an expiration date in AD, the default expiration date is 90 days – in the future, the help desk will specifically ask for start and end dates for the contractor and add the end date to AD. If the time frame is greater than one year the helpdesk will get approval from InfoSec for the extension. (Please refer to 3rd Party Non-HCHD Approvers knowledge document)
Verifying Current Access	Management in the user departments are required to review reports twice a year that show access authorized by their departments to employees and contractors, and communicate any necessary changes to access to IT.	The reports distributed in December 2013 did not include users not assigned to templates, and did not include IT employee users. Not including all users on the reports increases the risk that access no longer required will not be timely disabled.	IT Management should include users not assigned to templates, and IT employee users on reports sent twice a year to management to review and communicate necessary changes in access.	We agree with this recommendation. The summer attestation is wrapping up, the financial modules will be reviewing the non-template items as part of our cleanup. When this attestation is done, the CIO will also perform the Epic security attestation for the Epic users that are in I.T.

RISK ASSESSMENT AND SUMMARY OF RECOMMENDATIONS

The risk matrix below presents the assessed level of risk or exposure identified during our procedures. Inherent risk relates to factors that because of their nature cannot be controlled or mitigated by management. Inherent risk includes factors such as legislative changes, number and dollar amount of transactions processed and/or complex nature of transactions. Control risks relate to factors that can be influenced or controlled by management. Controls such as policies and procedures, electronic or manual approvals, system security access, and separation of job responsibilities may be instituted by management in order to mitigate control risk. Control risk is assessed during the planning phase in order to establish the nature, timing, and extent of testing and at the conclusion of the engagement in order to incorporate actions taken to implement our recommendations. The overall risk considers a combination of inherent and control risks.

Inherent Risk:	Control Risk:		Overall Risk:
<input checked="" type="checkbox"/> High <input type="checkbox"/> Moderate <input type="checkbox"/> Low	Prior to Procedures	After Procedures	<input checked="" type="checkbox"/> High <input type="checkbox"/> Moderate <input type="checkbox"/> Low
	Adequate	Adequate	
Type of Procedures: Audit			
Purpose: To evaluate critical controls for providing the appropriate level of user access to Epic financial modules, changing user access when necessary, and terminating user access that is no longer required.			
Outstanding Audit Recommendations:			
Priority Rating:	Audit Recommendations: Harris Health System		
1	Continue to provide leadership for developing and implementing templates and establish a target date for completing the assignment of templates to the 123 remaining users.		
1	Document procedures regarding changing user security settings in a formal written procedure signed by the Chief Information Officer, and distributed to all IT employees. Periodically review the Epic Change Logs to identify whether unapproved changes were made.		
1	Implement a process of assigning access to contractors with expiration dates that correspond to the anticipated length of time the outside contractor's services are expected to be required.		
1	Include users not assigned to templates, and IT employee users on reports sent twice a year to management in user departments to review and communicate necessary changes in access.		
Priority	1. Implement immediately (30 – 90 days) – Serious internal control deficiencies; or recommendations to reduce costs, maximize revenues, or		

Rating	improve internal controls that can be easily implemented. 2. Work towards implementing (6 – 18 months) – Less serious internal control deficiencies, or recommendations that can not be implemented immediately because of constraints imposed on the department (i.e., budgetary, technological constraints, etc.). 3. Implement in the future (two – three years) – Recommendations that should be implemented, but that can not be implemented until significant and/or uncontrolled events occur (i.e., legislative changes, buy and install major systems, requires third party cooperation, etc.).
---------------	--