UT SOUTHWESTERN
MEDICAL CENTER

Daniel K. Podolsky, M.D.
President
Philip O'Bryan Montgomery, Jr., M.D. Distinguished
Presidential Chair in Academic Administration

Professor of Internal Medicine
Doris and Bryan Wildenthal Distinguished
Chair in Medical Science

September 5, 2012

Kenneth Shine, M.D.
Executive Vice Chancellor for Health Affairs
The University of Texas System
601 Colorado Street
Austin, TX 78701

Enclosed for your information is a copy of the University of Texas Southwestern Medical Center Internal Audit Report 12:25 Epic Security Administration.

I concur with the auditors' recommendations. Four recommendations are in process of being implemented.

Sincerely,

Daniel K. Podolsky, M.D.

Enclosure

cc: Arnim E. Dontes
J. Michael Peppers
Eva Narten

5323 Harry Hines Blvd. / Dallas, Texas 75390-9002 / 214-648-2508 Fax 214-648-8690
www.utsouthwestern.edu

The University of Texas Southwestern Medical Center

Internal Audit Report 12:25
Epic Security Administration

September 5, 2012

Office of Internal Audit
5323 Harry Hines Boulevard
Dallas, Texas 75390-9017
(214) 648-6106

The University of Texas Southwestern Medical Center
Internal Audit Report 12:25
Epic Security Administration
FY 2012

AUDIT REPORT
September 5, 2012

Daniel K. Podolsky, M.D., President
The University of Texas Southwestern Medical Center
5323 Harry Hines Boulevard, MC 9002
Dallas, Texas 75390-9002

Dear Dr. Podolsky:

The University of Texas Southwestern Medical Center (Medical Center) Office of Internal Audit has completed its 12:25 Epic Security Administration audit as detailed below.

Executive Summary

The audit focused on Epic security administration for the period of September 1, 2011 to June 30, 2012 and a review of security classes, or functional roles, associated with the Epic Resolute Professional Billing (PB) application for appropriate segregation of duties as of March 19, 2012. The importance of the Epic suite in the user community resulted in this being a risk based audit on the fiscal year 2012 Medical Center audit plan. Our examination was conducted according to guidelines set forth by The University of Texas System Administration Policy UTS129 "Internal Audit Activities", the Regents' Rules and Regulations, and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.* To achieve the audit objectives, Internal Audit viewed training videos, reviewed manuals, conducted interviews, documented process flowcharts and performed control testing.

The audit found the control environment was not adequate with respect to user access for the Epic suite of applications and segregation of duties for the Epic Resolute Professional Billing (PB) application. To ensure adequacy, four recommendations were made to strengthen access controls and improve segregation of duties.

1. User Termination (Epic Suite) - 44 users identified as terminated had both active Epic and active network accounts. We recommended that these accounts be disabled immediately to control the risk of unauthorized access. To increase efficiency and effectiveness, management is also encouraged to disable 651 active Epic accounts belonging to terminated users, but whose network accounts have been appropriately disabled.
2. Segregation of Duties (Resolute PB Users) - Management should review security classes, or functional roles, for the Epic Resolute PB application to address excessive access granted to users.

3. User Access Recertification (Epic Suite) - To ensure users are monitored for appropriate access, procedures should be implemented to periodically recertify, at minimum, access to critical Epic applications.
4. Elevated User Access (Epic Suite) - Ability to administer security and move program changes to production should be removed from 59 users.

Background

The suite of applications from Epic Systems of Verona, Wisconsin comprises a majority of the systems supporting medical and billing operations for the Medical Center's hospitals and clinics. Security Administration for the suite is managed through a centralized database such that changes to a user's account can affect their access to all applications in the suite. The Technical Services group within Health System Information Resources (HSIR) manages the addition, deletion, and maintenance of all Epic users and the assignment of security classes, or functional roles. Configuration of those roles and the application functionality within those roles is performed by HSIR business analysts responsible for supporting each individual Epic application within the suite. The Epic suite is also integrated with Windows Active Directory such that termination of a user's access at the Windows network level effectively terminates their access to all Epic applications. A team of one supervisor and seven business analysts currently administers the 10,500 active Epic users within the suite.

Audit Objectives

The primary objective of this audit was to assess the control environment over Epic security administration for the Epic suite related to appropriate user access and segregation of duties for the Epic Resolute PB application.

Scope and Methodology

The audit scope included a review of the Epic security administration function for the period September 1, 2011 to June 30, 2012, as well as a review of security classes (functional roles) associated with the Epic Resolute PB application for appropriate segregation of duties as of March 19, 2012. Our examination was conducted according to guidelines set forth by The University of Texas System Administration Policy UTS129 "Internal Audit Activities", the Regents' Rules and Regulations, and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.*

To obtain an understanding of Epic security controls and the Medical Center's Epic security administration function, Internal Audit viewed Epic computer-based security training videos, reviewed Epic security manuals and conducted interviews with Systems and Operations, Systems Access Management (SAM) as well as HSIR Technical Services personnel. Process narratives and flowcharts, including relevant risks and controls, were documented, validated with both SAM and HSIR management and provided to management for future reference.

Control testing concentrated on three process areas:

- User termination - Using CAATs, we compared Epic user information with all terminated users in the HRMS system and their associated network accounts in the Windows Active Directory system to identify terminated users with active Epic accounts. One recommendation was made in this area (recommendation 1).
- Segregation of duties for the Resolute PB application - CAATs were also used in this area to extract and analyze Epic users and their assigned security classes (functional roles) and security points. We then met with the HSIR Business Analyst Supervisor supporting Resolute PB as well as the Associate Vice President for Faculty Practice Plan Billing Operations to confirm our conclusions regarding segregation of duties testing. One recommendation was also made in this area (recommendation 2).
- User setup - Computer-assisted audit techniques (CAATs) were used to select a random sample of Epic users for setup testing, comparing Epic user information with extracts from the Human Resources (HRMS) and Information Access Request (IAR) systems. No exceptions were identified in this testing, but one recommendation was made regarding monitoring (recommendation 3).

Follow-up testing of one issue noted by Deloitte during the FY12 AFR audit was also performed:

- This issue regarded segregation of duties for users granted elevated access. CAATs were used in this area to identify and report users with elevated access administer security or change Epic programs through the Data Courier application. One recommendation was made (recommendation 4).

AUDIT RESULTS/RECOMMENDATIONS

Our audit observations resulting in recommendations are detailed below:

1. **User Termination (Epic Suite)**

   Testing for terminated user access to Epic systems as of March 2012 revealed the following conditions:

   - 44 of 10,500 (.5%) active Epic user accounts were identified as belonging to terminated employees, fellows or non-employee associates. All 44 of these accounts also had current access to the network, permitting them unauthorized access to Epic systems as well as other Medical Center systems to which they are privileged. 38 of the 44 (86%) users had terminated from the Medical Center within the six months prior to March 2012.
   - 651 of 10,500 (6%) active Epic user accounts were also identified as belonging to terminated employees; however, their network access had been properly disabled. While this condition presents a relatively low risk of unauthorized access, it can result in decreased efficiency and effectiveness in maintaining accounts which are no longer needed. In addition, this type of situation has been cited as an exception by external auditors in prior audits. Per discussion with the HSIR Business Analyst Supervisor, this condition is primarily caused by business analysts determining the active status of personnel by searching for an active email account using their Outlook email client. However, this procedure is

unreliable since, due to Outlook's caching feature, it often indicates an email account is active even though it has been deleted due to termination.

Recommendation

a. Commensurate with the implementation of the PeopleSoft Human Capital Management (HCM) system, the Systems and Operations Group, in cooperation with Administrative Systems, will be implementing an interface to Active Directory that will automatically disable a user's network account when their status is updated to terminated in HCM. Management is encouraged to pursue implementation of this process as it will comprise a strong control for terminating user network access while also effectively terminating access to Epic. To control the present risk, HSIR Technical Services should work with the SAM group to ensure both network and Epic access is immediately disabled for the 44 users noted above.
b. It is recommended management consider dedicating resources to inactivate the 651 users noted above to increase efficiency and effectiveness.
c. Management should review and improve termination procedures as needed to prevent recurrence of these situations.
d. Due to concern for patient safety and quality of care, a user's Epic In-Basket messages must be evaluated and re-assigned in a timely manner before their Epic account can be disabled. Accordingly, we understand it is not feasible at this time to implement an automated process to disable a user's Epic account concurrent with disabling their network account. Therefore, it is recommended management improve existing manual processes by using the HRMS system and, once implemented, the HCM system to determine personnel status. The Intranet phone directory page at http://www.utsouthwestern.net/intranet/services /phone-directory.html can also be used for a quick status check since it is refreshed nightly from the HRMS system and will continue to be refreshed with HCM data after the conversion to HCM. Alternatively, once HCM is implemented and the interface to Active Directory discussed in (a) above is verified, a daily report of users terminated in Active Directory could be obtained. Finally, management is encouraged to continue to pursue a feasible automated solution to disable Epic accounts.

Management Response

a. We agree. As discussed in the recommendation above, the interface to Active Directory will be implemented effective with the implementation of HCM. To address the present risk, per discussion with SAM group management:
    - 28 of the 44 users noted above were inactivated subsequent to the cutoff date for the audit procedure and are no longer a risk.
    - 4 users have not yet been disabled due to a backlog in working Expired NEA reports. These accounts need to be researched in the HRMS system to determine if there are any pending appointments. If not, they will be disabled by 8/31/12.

- The expiration date for 1 contractor's user ID was erroneously extended and will be disabled by 8/31/12.
- The remaining 11 users will be researched and disabled by 8/31/12 if there are no pending appointments.

Implementation Status: In Process
Implementation Date: September 30, 2012

b. We agree, and work is in progress.

Implementation Status: In Process
Implementation Date: January 1, 2013

c. We agree. Epic Technical Services has been and will continue to work closely with the SAM group to tighten these processes.

Implementation Status: In Process
Implementation Date: March 31, 2013

d. We agree and are using the URL above. Thank you for bringing this to our attention. Once HCM is implemented, we will work with Administrative Systems to obtain the necessary information from HCM to determine personnel status, or pursue a report from Active Directory. Provided there is no deleterious effect on patient safety or quality of care, we will continue to look for a feasible automated solution to implement.

Implementation Status: In Process
Implementation Date: March 31, 2013

Responsible Personnel:
Assistant Vice President, Chief Technology Officer

2. Segregation of Duties (Resolute PB Users)

Access to the Epic Resolute PB application is granted by assigning users one of 42 security classes. A security class essentially equates to a functional role. An analysis of these 42 security classes as of March 19, 2012 revealed the following conditions:

a. Several instances of users granted excessive access for their job duties were identified. For example:
   - Access to override prices, discounts and DBI (do not bill insurance) was granted to numerous functions, not restricted to just billing managers
   - Access to maintain procedure codes was granted to numerous functions, not limited to just HSIR support staff
   - The MSRDP Document Control function was granted access to post payments and perform limited write-off of charges

- The MSRDP Payment Posting function was granted access to void and delete charges
- The MSRDP Finance function, which requires only read access, was granted numerous abilities to modify data including entering charges and payments, deleting charges and overriding prices.

b. Several security classes with only minor variations were configured for the billing manager function in various clinical departments. Per discussion with the Associate Vice President for Faculty Practice Plan Billing Operations, this condition is a departure from the original strategy upon installation to have only one billing manager security class and may be needlessly complicating security administration.

Recommendation

a. MSRDP Billing Operations management should work with support staff in HSIR to review all Resolute PB security classes and ensure access is granted according to the principle of least privilege required to perform job duties.
b. To simplify security administration, variations in security classes for similar functions, such as billing managers, should be eliminated in favor of a common functional class wherever possible.

Management Response

a. MSRDP Billing Operations management will coordinate meetings with HSIR during September and October 2012 to review security classes and ensure access is correct for the required job duties
b. As part of the meeting above, MSRDP will work with HSIR to evaluate security classes and combine if possible.

Implementation Status: In Process
Implementation Date: November 1, 2012

Responsible Personnel:
Associate Vice President for Faculty Practice Patient Financial Services

3. User Access Recertification (Epic Suite)

Procedures are not in place to periodically re-certify user access to Epic modules to ensure it is appropriate. Without such monitoring, users could be granted excessive access without detection, which could result in activity such as deleting or voiding patient charges or writing unauthorized prescriptions. Evidence of such reviews was requested by Deloitte for the FY12 AFR audit as part of their IT general controls testing, but could not be provided.

HSIR Technical Services management should implement procedures to periodically but at least annually, re-certify user access to Epic modules. If it is not possible to include all modules, the scope of this review should include, at least, critical modules, such as EpicCare, Resolute PB and the new Resolute Hospital Billing,

which will be implemented in August 2012. This review should comprise documented verification and sign-off by user management that users are assigned the appropriate security class as well as documented verification and sign-off by system owners that security classes are configured to grant users the minimum access necessary for job duties. Evidence of such documented reviews should be retained for external or internal auditor inspection.

Recommendation

HSIR Technical Services management should implement procedures to periodically, but at least annually, re-certify user access to Epic modules. If it is not possible to include all modules, the scope of this review should include, at least, critical modules, such as EpicCare, Resolute PB and the new Resolute Hospital Billing, which will be implemented in August 2012. This review should comprise documented verification and sign-off by user management that users are assigned the appropriate security class as well as documented verification and sign-off by system owners that security classes are configured to grant users the minimum access necessary for job duties. Documentation of such reviews should be retained to support the work completed.

Management Response

The Chief Technology Officer has asked the HSIR Development team to create a web-based system to automate an annual Epic user recertification process. The system will match Epic users to a database of their respective departmental contacts as supplied by Administrative Systems. An email will be sent annually to these contacts prompting them to login to the system, review a listing of their employees with Epic access and their type of access and attest to the continuing need for their employees to have this access with a Yes/No response. The system will track responses in a database and facilitate follow-up with non-responders to ensure completeness. Procedures will be implemented to monitor responses and implement changes to Epic user security as requested by the departmental contacts. The current estimate for completion of the application is January 1, 2013.

Implementation Status:	In Process
Implementation Date:	January 1, 2013

Responsible Personnel:
Assistant Vice President, Chief Technology Officer

4. Elevated User Access

Follow-up testing of one issue noted by Deloitte during the FY12 AFR audit was also performed. Testing of users with elevated privileges to Epic applications as of June 25, 2012 revealed 59 users who no longer needed global access to the Data Courier application that would enable these users to administer Epic security as well as move changes to production for all Epic applications. Four (4) of the 59 users were HSIR Business Analysts who do not require this level of access for their current job

duties. Fifty-five (55) of the 59 users were Epic Systems remote vendor support personnel. Previously, in order to take full advantage of the Epic support model of 24 hours, 7 days a week for system provision help, the 55 named users were required. Epic has recently changed its support model into an integrated cross-trained smaller team that is still able to support all the modules across the Epic suite. Based on this change, per discussion with the Senior Information Resources Manager in HSIR Technical Services, these Epic Systems vendor staff no longer need this level of access. They may perform changes in the test (POC) environment, but HSIR Technical Services staff would move them to the production (PRD) environment after going through Change Control procedures.

Recommendation

Management should remove the unnecessary global access from these users immediately to mitigate the risk of unauthorized changes to the security or programs in the production environment. Implementation of a periodic access recertification process as recommended separately (recommendation 3) in this report will help to reduce recurrence of this condition.

Management Response

We agree with the finding and recommendation. We have remediated the issue with the identified accounts.

Implementation Status:	In Process
Implementation Date:	August 31, 2012

Responsible Personnel:
Assistant Vice President, Chief Technology Officer

Conclusion

The audit found the control environment was not adequate with respect to user access for the Epic suite of applications and segregation of duties for the Epic Resolute Professional Billing (PB) application. To ensure adequacy, four recommendations were made related to user termination (Epic Suite), segregation of duties (resolute PB Users), user access recertification (Epic Suite) and elevated user access (Epic Suite).

We appreciate the courtesy and cooperation of all staff within HSIR and Faculty Practice Patient Financial Services.

Andrea Claire, JD, MBA, CIA - Manager of Internal Audit
Jeffrey Kromer MBA, CPA, CISA, CBA, CFSA - Supervisor of Internal Audit

600 Audit Hours Expended

Sincerely,

Eva Narten, CPA, CIA, CISA
Director *ad interim* of Internal Audit

Cc: Arnim E. Dontes, MBA, Executive Vice President for Business Affairs
Kirk Kirksey, Vice President for Information Resources, Chief Information Officer
Suresh Gunasekaran, Associate Vice President for Health System Information Resources
Dennis Pfeifer, Assistant Vice President and Chief Technology Officer for Health System Information Resources
Bruce Fairbanks, CPA, Vice President for Health System Financial Affairs
Kelly Kloeckler, Associate Vice President for Faculty Practice Patient Financial Services