MEMORANDUM

TO: Donna K. Sollenberger, MA
   Executive Vice President and CEO, UTMB Health System

   Todd A. Leach
   Vice President and CIO, Information Services

FROM: Kimberly K. Hagara, CPA, CIA, CISA, CRMA
      Associate Vice President, Audit Services

DATE: January 31, 2014

SUBJECT: utmbConnect General Computer Controls
          Audit Control Number 2014-026

Attached is the final audit report regarding the utmbConnect General Computer Controls. This audit will be presented at the next Institutional Audit Committee meeting.

Additionally, please find attached Audit Services audit recommendation follow up policy. Each of the recommendations is classified by type at the end of its identifying number: Significant (S), Risk Mitigation (R), or Process Improvement (P). As you will note in the policy, the classification of the recommendation determines the frequency of our follow up. All follow up results are reported quarterly to the Institutional Audit Committee.

Thank you for your cooperation and assistance during the course of this review. If you have any questions or comments regarding the audit or the follow-up process, please feel free to contact me at (409) 747-3277.

Attachment

c: Rex M. McCallum, MD
   Mark S. Kirschbaum, RN, PhD
   George H. Gaddie
The University of Texas Medical Branch
Audit Services

Audit Report
utmbConnect General Computer Controls
Audit Control Number 2014-026
January 2014
Background
In 2003, The University of Texas Medical Branch (UTMB Health) began the initial phases of implementing the Epic electronic medical record system to improve quality of patient care, patient safety, and operational efficiency. In early 2013, UTMB Health implemented the integrated Epic Patient Access and Revenue Cycle application modules commonly referred to as utmbConnect. These modules further extended UTMB Health’s goal of better and safer patient care, a single electronic medical record containing all information about a patient’s care, and a single patient billing statement that includes all hospital, clinic, and provider charges.

General computing controls consist of processes for managing the environment within which major information systems such as Epic are developed, maintained, and operated. These controls relate to security management, configuration management, access management, segregation of duties, and contingency planning. As UTMB Health continues to move towards the increased use of the Epic electronic medical record system, establishing adequate and consistently applied controls becomes essential in preventing unauthorized access, use, disclosure, disruption, modification, or destruction of the Epic application or its data.

Audit Objectives
The primary audit objective is to assess the general computing controls of the Epic application modules and supporting utmbConnect system components.

Scope of Work and Methodology
Our scope of work primarily included an assessment of general computing controls but also incorporated related application and business process controls, particularly as they relate to recent utmbConnect changes within the Epic electronic medical record system.

The audit methodology included a review of relevant policy and practice standards, training, security risk assessments, vulnerability scans, operational processes and procedures, tools, logs, and data repositories. We reviewed independent consulting assessments, previous external audits, and related initiatives in progress. Additionally, we conducted interviews with a broad group of key stakeholders, including UTMB Health business operations and technical support, and external auditors.

The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing as promulgated by the Institute of Internal Auditors.

Audit Results
Security Management
Security management establishes a framework and continuous cycle of activity for assessing risk, monitoring the adequacy of computer related controls, and developing and implementing effective security procedures. Weaknesses in security management can result in inadequate assessment of and response to information security risks related to the applications and systems on which they depend, as well as significantly increase the risk that required controls are not consistently applied. Key elements of security management include conducting periodic risk assessments, testing and remediation of information security vulnerabilities, establishing practice standards, problem management, data encryption, and proper media disposal.

Risk Assessments
Risk assessments should consider risks to data confidentiality, integrity, and availability, and the range of risks to which the application and data may be subject. As observed, key stakeholders periodically assess Epic risks, with follow-up conducted by the Office of Information Security to verify the remediation of related security deficiencies. To ensure
third party services are adequately secure, the Office of Information Security continues to mature the third party risk assessment process.

**Vulnerability Tests**
Periodic scans of and updates to software protect against known system vulnerabilities. Our review confirmed Information Services (IS) Network and Security Operations periodically perform vulnerability scans of UTMB Health information systems. We noted that the scans included approximately 200 devices supporting utmbConnect and confirmed that high and critical risks were generally remediated. Although these scans did identify multiple occurrences of a single high-risk vulnerability, this was identified as a constraint of the current Epic version and will be resolved with the next versioning upgrade planned for Spring 2014. In the interim, compensating controls are established to reduce the vulnerability to an acceptable risk level. Additionally, during our review it was determined that the institutional server inventories primary data source (STEAM) is not accurate, complete, or current.

**Recommendation 2014-026-01-P:** IS should update or revise the primary data source for the current server inventory listing. Additionally, IS should establish operational controls to ensure the continued maintenance of a reliable server inventory.

**Management’s Response:** Information Services will update the data source for the current server inventory and implement a new process to ensure the continued maintenance of a reliable server inventory.

**Implementation Date:** December 31, 2014

**Practice Standards**
The UTMB Health Information Resources Practice Standards provide the operational detail required for the successful implementation of the Information Resources Security program. Any exception, with a business case justifying the exception, requires formal assessment and approval by the Information Security Officer. Audit Services identified several Epic generic accounts providing group use that were missing the required documentation.

**Recommendation 2014-026-02-P:** IS should submit the required exception requests for the identified generic accounts with supporting justification to the Information Security Officer for formal assessment and approval.

**Management’s Response:** Information Services will review the need for each generic account and, if we retain each, will submit a request to the Information Security Officer for approval.

**Implementation Date:** April 30, 2014

**Problem Management**
Problem Management includes the activities required to diagnose the root cause of incidents identified through the Incident Management process. Consistent with industry best practices, resolutions are identified to prevent future incidents and minimize the impact of incidents that cannot be prevented. As observed, the information security team, as well as Epic application teams and technical services, are actively engaged in these processes.
Data Encryption
Data encryption prevents the unauthorized access to and disclosure of confidential data. Encryption initiatives to protect confidential information either are completed or are in progress to provide encryption capabilities for wireless, email, laptops, backups, Smart devices, and removable media such as USB flash drives.

Media Disposal
Media disposal guidelines prevent inadvertent data disclosures by ensuring removal of all data prior to the sale, transfer, or disposal of institutionally owned information resources and associated data storage devices when production systems are decommissioned. Our review noted media disposal practices undergo periodic testing and follow institutional guidelines.

Configuration Management
Configuration management provides reasonable assurance that configuration and operation of system hardware and software is secure and functions as intended throughout the product life cycle. In addition, only authorized changes to information system resources occur and that all appropriate parties receive notification of potential changes, both scheduled and unscheduled. Weaknesses in configuration management can result in unauthorized modifications or additions to the applications and to system components, leading to unauthorized access to data and applications. Configuration management involves the removal of unnecessary services, automated logoff due to inactivity, generating adequate audit trails, maintaining vendor supported product versioning, and change management.

Unnecessary Services
The integrity, confidentiality and availability of Epic data rely upon appropriate services operating securely within the system. Removal of unnecessary services from the Epic platforms helps ensure they continue to deliver data in a secure and reliable manner. Overall, vulnerability scans substantiated the removal of unnecessary services, continued maintenance of vendor patches, and default passwords for administrator accounts changed as required. Additionally, operating systems at risk have automated anti-virus updates in place and the training and test environments do not have production data containing patient identifiable information.

Automated Logoff
When idle, information systems should initiate an automated logoff requiring the user to reestablish access using appropriate identification and authentication procedures. Although an automated logoff occurs after a predetermined period of inactivity, the UTMB Health Information Resources Practice Standards requirement is ten minutes while the corresponding setting within Epic is 20 minutes. To maintain best practices as commonly specified for the healthcare industry, UTMB Health should adopt 15 minutes as the institutional practice standard and configure the Epic logoff setting in accordance with the revised practice standard.

Recommendation 2014-026-03-R: The Information Security Officer should revise practice standards to reflect healthcare industry best practices concerning automated logoff after 15 minutes of inactivity, and the Epic logoff setting should be reconfigured accordingly.

Management’s Response: The Information Security Officer will update the Physical Access practice standard to reflect that automated logoffs will occur after 15 minutes of inactivity. The Epic session time-out settings will be reconfigured to 15
utmbConnect General Computing Controls Audit
Audit Control Number 2014-026

minutes.

Implementation Date: March 30, 2014

Audit Trails
All production application systems storing confidential data should log privileged use and ensure user accountability. As observed, audit logging does occur, capturing a variety of access and security event activity. While continuing to mature, these logs have generally satisfied investigative and monitoring needs to date.

Product Versioning
Product versioning maximizes system availability and enhances user functionality through continued vendor support. Epic software maintenance, upgrades, and enhancements occur timely, with the next Epic versioning upgrade planned for Spring 2014.

Change Management
Change Management controls establishes a formal process to ensure review, impact analysis, testing, approval, and notification prior to system or application changes in the production environment. Additionally, controls include subsequent tracking and assessment, and include provisions for emergency changes. Our review included sampling and reconciling Customer Service Requests pertinent to corresponding utmbConnect change management tickets with no exceptions noted.

Access Management
Access management controls help secure information resources by permitting or denying user access as well as governing its use, thereby protecting them from unauthorized modification, loss, and disclosure. For access controls to be effective, they require proper approval, implementation, and maintenance. Weaknesses in access controls can result in unauthorized access to and modifications of applications, related controls, data, or system components. Key elements of access control include account management, establishing rules for vendor and remote access, authentication procedures, disabling inactive accounts, and physical security.

Account Management
Establishing accountability for the usage of information resources is critical to an overall information security program. As observed, the IS Access Management team manages Epic access requests using the IBM Tivoli Identity Management (ITIM) system. ITIM documents requests and corresponding approvals, which are contingent upon the completion of related training. There are approximately 7300 unique Epic user accounts identified within ITIM, assigned to over 100 unique roles with corresponding utmbConnect training. These combined safeguards result in minimizing common risks associated with unauthorized access to and use of the Epic applications. Specific to individual users associated with utmbConnect, Nondisclosure Agreements, which help to initiate the access provisioning process, were tested for 46 contractors, vendors, consultants, analysts, or application specialists each of which were documented within ITIM as required.

Vendor Access
Vendor accounts should remain disabled except when in use for authorized maintenance. As observed, the IS Operations Command Center manages the escrowed passwords for Epic on-call accounts; however, the physical lengths of the escrowed passwords were non-compliant with UTMB Health Information Resources Practice Standards when initially tested. Subsequently, the escrowed Epic on-call passwords were reset during the course of the audit
to satisfy password composition requirements.

Remote Access
In accordance with established institutional practice standards, secured remote access to UTMB Health information resources is available to support related business functions. Users needing remote access receive approval through the ITIM access management provisioning process, which requires an active UTMB Health domain username and password. The Epic application authenticates these user credentials to connect to and conduct normal business functions from remote locations.

Authentication Procedures
User authentication is a means to control who has access to an automated information system. Users have their own unique IDs and passwords to access the Epic application. This practice helps limit unauthorized use of the Epic application by restricting the access privileges of each user and increases individual accountability through the occurrence of logging and monitoring activities. Individual usernames and passwords used by the Epic application to authenticate users are generally consistent with applicable UTMB Health Information Resources Practice Standards.

Inactive Accounts
Access to, change to, and use of UTMB Health information resources must be strictly secured. Information access authority reviews for each user should occur on a regular basis, as well as each job status change such as a transfer, promotion, demotion, or termination of service. To ensure the timely removal or disabling of Epic user accounts due to role change or separation, the Epic security team recently assessed procedures for removal of inactive accounts for potential process improvement. The UTMB Health Information Security and Privacy Compliance Committee reviewed and approved implementation of the resulting recommendation introducing more efficient and effective operational controls. Our review did note the access review of privileged contractor or vendor accounts is typically associated with the annual expiration date of the corresponding Nondisclosure Agreement. To maintain best practices as commonly specified for the healthcare industry, IS should evaluate implementing a quarterly review of these accounts to ensure a more timely review and removal of privileged or special access.

Recommendation 2014-026-04-P: IS should evaluate a quarterly review of privileged accounts to reflect healthcare industry best practices, revising the expiration of nondisclosure agreements and related practice standards accordingly.

Management’s Response: Information Services will evaluate a quarterly review of privileged accounts and will revise the expiration of non-disclosure agreements and related practice standards where appropriate.

Implementation Date: March 1, 2014

Additionally, a formal project team comprised of Human Resources, Legal Affairs, IS Access Management, the Office of Information Security, and the Office of Institutional Compliance is forming to address how to best manage access privileges for individuals on extended leave.

Physical Security
Appropriate safeguards should be in place to restrict access to non-public areas and facilities where information resources physically reside. As observed, physical access to critical
information technology devices and systems is secure and related controls are functioning as intended.

**Segregation of Duties**
Segregation of duties refers to the policies, procedures, and organizational structures that help ensure no single individual can independently control all key aspects of a process or computer related operation and thereby gain unauthorized access to information resources. Individuals should not have any access to the application, data, or the operating system beyond that which they need to perform their assigned job duties. Weaknesses in segregation of duties can result in unauthorized access to applications, data, or system components. In addition, such weaknesses can circumvent management intentions allowing control overrides to occur. Key elements of proper segregation of duties include the principle of minimum necessary, adequate restrictions of privileged use, proactive monitoring of access activity, and periodic reviews for the continued appropriateness of access.

**Minimum Necessary**
The access privileges of all users, systems, and programs must be restricted based upon the concept of 'minimum necessary' use (i.e., users receive only those access privileges minimally required to perform their assigned job duties). Generally, the Epic application configuration ensures access privileges are segregated (364 active profiles, 142 security classes) such that users or processes acting on behalf of users obtain only the necessary privileges to accomplish authorized tasks relevant to assigned roles. However, Nordic Consulting (a UTMB Health Business Partner) recently concluded that Epic's security implementation strategies and configuration choices are dated and implementation of newer Epic features would maintain best practices. Implementation of the resulting recommendations to better define users and provision access consistent with best practices is in progress. These enhancements will not only optimize security administration and provide greater efficiencies, but will also further standardize Epic access privileges thereby strengthening the technical enforcement of minimum necessary.

**Privileged Use**
Technical support staff, security administrators, system administrators, and others may have special access account requirements (privileged use) as compared to typical or normative users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling, and monitoring these accounts is extremely important to an overall information security program. Additionally, all user accounts created must have an associated request and approval appropriately documented within the ITIM system. Special privileges from a system perspective are limited to a minimal number of individuals; however, access as currently granted for these system administrators varies broadly within the team and access authorization approvals are not consistently documented using ITIM. Although there was no indication of inappropriate access, reassessment of team member privileges and verification of appropriate authorization in the ITIM system should occur to ensure staff is performing only authorized duties relevant to their respective job duties.

**Recommendation 2014-026-05-R:** IS should conduct a review of special access privileges for consistency and continued appropriateness based upon business need, and verify appropriate documentation within ITIM.

**Management’s Response:** Information Services will review the special access privileges for consistency, appropriateness and business need and properly document these within ITIM.
Implementation Date: May 1, 2014

Additionally, our review included privileged users from an applications perspective. Fifty-five access accounts comprising individual users, generic accounts, and processes acting on behalf of users were tested. There was no indication of inappropriate access.

Proactive Monitoring
Fundamental to healthcare regulations and security standards is the expectation of logging and auditing to identify questionable access activity, assess security programs, and respond to potential system weaknesses. As observed, audit trails containing pertinent user and event data are typically sufficient to satisfy not only investigative inquiries regarding Epic usage, but proactive monitoring as well. Combinations of monitoring functions are associated with Epic and independently reviewed. The Office of Compliance routinely monitors access activity associated with Epic use, which captures both system and patient data level (application) activity while the Office of Information Security monitors information security events and network data transmissions.

To protect confidential patient information and demonstrate due diligence, UTMB Health examines user access activity based upon areas of prioritized risk. The primary automated solution used to detect a potential patient privacy incident is FairWarning. In addition to the standard classifications of access activity currently monitored by the Office of Institutional Compliance, three areas of concern were also reviewed for potential misuse; non-clinical staff, dual roles (employee and student), and Texas Department of Criminal Justice staff. Ninety-four individuals with secretarial or administrative coordinator titles have “admin assistant” access to patient data within Epic. Of these, 13 individuals were tested, one of which indicated potentially inappropriate access requiring a standard investigative review. The Office of Institutional Compliance has this review in progress. As an added level of security, utilization of Epic’s “Break the Glass” feature could prompt these particular users with a warning that their actions will be audited. These additional monitoring capabilities would help ensure assigned access privileges support business process objectives.

Recommendation 2014-026-06-R: IS should evaluate the functionality of Epic’s “Break the Glass” for individuals granted “admin assistant” access privileges.

Management’s Response: IS collaborated with Compliance during the utmbConnect project to evaluate the “Break the Glass” (BTG) functionality in the Epic system and it was determined that implementation within the Connect project was a large effort and further action was deferred. A review of Epic’s new BTG functionality in their 2012 release will be conducted to identify desirable features, scope, and next steps towards implementation.

Implementation Date: April 1, 2014

Two hundred sixty-two individuals with Epic access were identified as having both student and employee roles. Of these, twelve individuals were tested, one of which indicated potentially inappropriate access requiring a standard investigative review. The Office of Institutional Compliance has this review in progress. As observed during the preliminary review, this individual had numerous instances of “self-access” (i.e., viewing one’s own information) which is an emerging trend for individuals associated with non-compliant Epic access, regardless of role. As an added level of security, a high-volume “self-access” filter
could potentially provide additional monitoring capabilities and ensure assigned access privileges support business process objectives.

**Recommendation 2014-026-07-R:** The Office of Institutional Compliance should evaluate the benefits of additional FairWarning filtering capabilities to detect high volume “self-access” as a potential indicator of non-compliant access.

**Management’s Response:** The Office of Institutional Compliance (OIC) will use FairWarning alerts to evaluate the correlation between high volumes of self-access and inappropriate access of other individuals’ Epic medical records. If the trend is substantiated the OIC will implement a FairWarning alert that monitors for a high-volume of self-access. Based upon individuals identified in the self-access alert, OIC will review a random sample on a weekly basis to determine whether any of these individuals have engaged in inappropriate access of Epic medical records.

**Implementation Date:** August 1, 2014

Additionally, testing also included a review of access activity for Texas Department of Criminal Justice staff and there was no indication of inappropriate access.

**Continued Appropriateness**
Privileged commands must be traceable to specific individuals by using comprehensive logs. Using these logs, a review of accounts with local administrator (root) access occurred to ensure job duties are appropriately segregated and needed. As observed through a comparison of logs, when migrating to the new production database, local accounts initially created for development or test purposes in the original database were not brought forward. Additionally, review of these accounts further ensured patient identifiable information had not been accessed within the Epic applications.

Review of Epic end user accounts occur semi-annually for continued appropriateness. The primary intent of this review is to ensure appropriate management of changes in roles, transfers, and separations. If access privileges inadvertently remain active within the Epic application, this review allows for detection and corrective action.

**Contingency Planning**
Contingency planning controls ensure that when unexpected events occur, critical operations continue without disruption or promptly resume, and critical and confidential data remains protected. If contingency planning controls are inadequate, even relatively minor interruptions can result in the loss of application data, which can cause financial losses, expensive recovery efforts, inaccurate or incomplete information, or the unavailability of critical applications. Key elements of continuity planning include system classification through business impact analysis, critical data backups, regular review and testing of disaster recovery plans with needed revision, and accessibility of copies of these plans during an event.

**System Classification**
Based on criticality and institutional significance, prioritized recovery objectives are determined through performing a business impact analysis. As part of the overall Epic business continuity plan, a business impact analysis has been completed and formally documented. Epic is classified as an institutionally significant information technology (IT) system.
utmbConnect General Computing Controls Audit
Audit Control Number 2014-026

Critical Backups
Formal backup procedures help prevent data loss and enable the recovery of systems and applications in the event of natural disasters, system failures, data entry errors, or system operations errors. Backups of pertinent data and software critical to the Epic system occur on a regular basis. Additionally, these backups are retained off-site.

Regular Review
Documented and tested plans help ensure recoverability of critical systems and data. Consistent with UTMB Health Business Continuity Planning Policy and Information Resources Practice Standards, we noted Business Continuity Plans and Disaster Recovery Plans exist for Epic. However, the current plans do not reflect critical changes to the Epic system subsequent to completion of the utmbConnect project, or the results of recent testing. To minimize and best manage the consequences of an event that interrupts critical business processes, it is essential these plans are accurate, complete, and current for staff to support recovery of the system and data.

Recommendation 2014-026-08-R: IS should update the existing Business Continuity Plans and Disaster Recovery Plans for Epic with recent changes and recovery testing results. Additionally, IS should establish operational controls to ensure the continued maintenance of reliable business continuity/disaster recovery plans.

Management’s Response: The business continuity and disaster recovery plans for Epic will be updated to reflect recent Epic changes and recovery testing results. IS will establish proper controls to ensure the continued maintenance of these plans. The controls will include an escalation process to ensure that leadership is notified when plans are outdated.

Implementation Date: May 31, 2014

Reliable Accessibility
To prevent the potential loss of information and ensure accessibility and timely recovery during an event, copies of the business continuity and disaster recovery plans are maintained in an institutionally shared central repository. Although dated, a copy of the plans is easily and reliably accessible during any event that may potentially cause a disruption in business functions.

Conclusion
UTMB Health implemented a new Patient Access and Revenue Cycle system, known as the utmbConnect project, replacing the previous legacy systems, streamlining processes, and increasing efficiency. Overall, controls for security management, access management, configuration management, segregation of duties, and continuity planning are functioning as intended within the areas reviewed for the Epic application. While numerous safeguards are in place and initiatives are in progress to enhance existing controls, additional opportunities for improvement include reliable server inventories, consistent assessment of practice standards exceptions, best practices concerning automated logoff and maximum expiration of contractor nondisclosure agreements, reassessment of privileged access, enhancements to monitoring strategies, and regular review of needed revision of business continuity plans.
We greatly appreciate the assistance provided by the Office of Institutional Compliance, Revenue Cycle Solutions, and the various staffing areas within Information Services and hope that the information presented in our report is beneficial.

Kimberly K. Hagara, CPA, CIA, CISA, CRMA
Associate Vice President, Audit Services

Randal J. Crawford, CISSP, CIA, CISA, CRISC, CGEIT
IT Audit Services Manager