August 29, 2013

ED BABAKANIAN
Chief Information Officer
Health Sciences Enterprise
8983

ADAM LYDDANE, PharmD
Chief of Clinical Applications
8935

BRIAN CLAY, M.D.
Interim Chief Medical Information Officer
8485

Subject: ***Epic EHR User Access Management***
Audit & Management Advisory Services Project 2013-13

The final audit report for Epic EHR User Access Management, Audit Report 2013-13, is attached. We would like to thank Clinical Application Support Team personnel for their cooperation and assistance during the review.

Because we were able to reach agreement regarding corrective actions to be taken in response to the audit recommendations, a formal response to the report is not requested.

The findings included in this report will be added to our follow-up system. We will contact you at the appropriate time to evaluate the status of the corrective actions. At that time, we may need to perform additional audit procedures to validate that actions have been taken prior to closing the audit findings

UC wide policy requires that all draft audit reports, both printed and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS personnel, or destroy them at this time. AMAS also requests that draft reports not be photocopied or otherwise redistributed.

David Meier
Assistant Vice Chancellor
Audit & Management Advisory Services

Attachment
cc: M. Baggett
D. Brenner
J. Hansen
M. Hansen
G. Matthews
B. Smith
S. Vacca
P. Viviano

UC San Diego

AUDIT & MANAGEMENT ADVISORY SERVICES

Epic Electronic Health Records
User Access Management
August 2013

Performed By:

Nai Hwang, Auditor
Terri Buchanan, Manager

Approved By:

David Meier, Assistant Vice Chancellor

Project Number: 2013-13

Table of Contents

I. Background

Audit & Management Advisory Services (AMAS) has completed a review of systems and processes used to manage user access to the Epic electronic health record system in accordance with the Fiscal Year 2012-13 audit plan. This report summarizes the results of our review.

The federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires that health care providers implement safeguards to ensure the privacy of protected health information (PHI). Over the past 10 years, related federal health care regulations, such as the Health Information Technology for Economic and Clinical Health (HITECH) Act, have promoted a transition from paper to electronic health records (EHR) to make medical records available to treating physicians and other providers regardless of their physical location. The Center for Medicare and Medicaid Services has also implemented financial incentive programs, such as Meaningful Use, to encourage physicians to move from a paper to an electronic environment. When patient health records are maintained in an electronic environment, processes for managing user access to patient information must be robust and consistent to ensure regulatory compliance, and also ensure the accuracy and completeness of data in the EHR.

UC San Diego Health System (UCSDHS) management has selected and is implementing the Epic system. Epic offers an integrated suite of health care applications centered on a hierarchical object-oriented database system. All Epic applications leverage the same central database, and Epic data can be queried using built-in reporting tools for research and other analyses.

Epic provides the functionality to document visit findings; enter test orders; prescribe medications; and capture charges based on established user profiles. Physicians and staff also access Epic applications to view visit schedules, patient demographic information, past medical history and problem lists, as well as medical procedure reports and results.

Epic has been implemented in the majority of outpatient locations and in the inpatient environment, making Epic the integrated system for creating and sharing clinical information. As of June 2013, UCSDHS has approximately 12,000 active Epic users including providers, medical staff, medical students, business staff, and some affiliates.

In the late 2011, the UCSDHS Steering Committee approved the implementation of Epic Revenue Cycle applications to achieve full integration of scheduling, registration, charge capture and professional/hospital billing functions into the clinical information system. Epic Revenue Cycle applications are scheduled to go live in October 2013. The UCSDHS Epic Project Team and UCSDHS Information Services have provided joint oversight of the Epic implementation. The Clinical Application Support Team (CA Support Team) oversees Epic user access activities.

II. Audit Objective, Scope, and Procedures

The objective of our review was to evaluate the effectiveness of Epic user access management processes.

We performed the following audit procedures to achieve the project objective:

- Reviewed relevant Epic guides and UC policies;
- Interviewed Ambulatory Clinical Applications personnel to gain an understanding of user access management procedures;
- Reviewed CA Support Team desk procedures;
- Interviewed personnel in the Graduate Medical Education, Medical Education and Medical Staff Administration Offices to discuss their processes for requesting Epic access for post doctoral students and medical staff;
- Met with campus Human Resources personnel to discuss the new hire information provided to the CA Support Team used to grant system access;
- Discussed the terminated employee notification process with Health System Payroll Office personnel;
- Identified unique Epic user groups and flowcharted the general process for requesting Epic access for those groups (***Attachment A***);
- Obtained Epic user data files from the UCSDHS Decision Support Team, and performed an analytical review to verify data completeness and identify user demographics;
- Analyzed two staff Termination Lists selected judgmentally to confirm that Epic access was terminated timely for separated employees; and
- Met with campus Administrative Computing & Telecommunications (ACT) personnel to gain an understanding of the identity management services provided by its Middleware & Identity Management Department.

The audit work performed was limited to evaluating Epic system user access management. We did not evaluate Epic access template content or change management procedures during this review. Epic template structure and content will be assessed in a separate Fiscal Year 2013-14 project.

III. Conclusion

Based on our review procedures, we concluded that some Epic access management practices needed improvement to help ensure the confidentiality, integrity and availability of PHI.

Audit tests performed to assess the process for removing Epic access for separated employees identified no exceptions. However, we identified opportunities for process improvement by standardizing access request procedures and data requirements; and eliminating duplicate and generic user accounts to the greatest extent possible.

These issues are discussed in more detail in the remainder of this report.

IV. Observations and Management Corrective Actions

A. Epic User Access Management

Data provided on Epic user access request worksheets was not standardized.

University Policy BFB-IS-11, *Identity and Access Management* (IAM) provides guidelines for creating an IAM structure that ensures the confidentiality, integrity, and availability of electronic information. IAM is based on the following principles and control objectives:

- Ensure unique identification of members of the University community and assignment of access privileges.
- Allow access to resources only by authorized individuals.
- Ensure periodic review of membership in the community and review of their authorized access rights.
- Maintain effective access mechanisms through evolving technologies.

Epic User Groups and Access Request Procedures

A standard request form and instructions for submitting multiple user access requests had not been developed. Therefore, UCSDHS offices submitted user access request worksheets they developed to the UCSDHS Information Services (IS) Customer Support Team. IS initiated the process by validating user information provided, and assigning a userid to all new personnel. The worksheets were then forwarded to the CA Support Team. The CA Support Team reviewed each user request, verified user identity, and if needed, manually added missing data found in other systems to complete the user profile. The requesting offices and major categories of active Epic users are listed in the table below.

UCSD Offices	User Role	Relationship with UC San Diego	Access Termination Date Entered	Related Database Source	Estimated Number of Users
Medical Staff Administration	Physicians and Non-physician providers	Employee	No (a)	PPS/PCIS	4,000
Graduate Medical Education Office	Post Graduate Students, Fellows, and Residents	Employee	No (a)	PPS/PCIS	1,700
Medical Education Office	Medical Students	Student / Employee	Yes	ISIS/PPS	600
UCSDHS Human Resources	Medical and Business Staff	Employee	None (a)	PPS/PCIS	4,000
Various Departments	Affiliates –Temporary Staff and Contractors (Traveler RNs, Research Associates, Volunteers, or Vendors	Contractor/ Volunteer	Yes, for some users	Variable based on role or contract terms	Not available
Various Departments	Business Operations Staff	Employee	No (a)	PPS/PCIS	Not available

Potential high risk users based on the absence of an employment relationship with UC San Diego.

(a) A termination date is not entered for career employees; but is entered for employees with appointment end dates and for temporary staff.

PPS - Campus Payroll Personnel System; PCIS - Patient Care Information System; ISIS – Integrated Student Information System

In addition to receiving Epic access requests via IS, the CA Support Team receives the New Employee Orientation (NEO) worksheet from campus Human Resources on a bi-weekly basis to obtain additional information for newly hired or transferred staff. ***Attachment A*** provides an overview of the sources and format of Epic access requests; and the general process work flow.

We reviewed the content of the various access request worksheets and found that that the data fields were not standard. In addition, some data fields, including DOB and SSN Last 4 fields were null for a number of accounts; and an appointment end date was not always provided for temporary employees, medical students, or affiliates. A null entry in a data field may be appropriate if the information is not pertinent to the individual account. However, information that helps to verify user identify, or that is key to granting or removing access should be populated. The adoption of required standard data fields would improve the effectiveness of the access management process.

Training

All users are required to complete Epic training prior to being granted access to the system. The training content varies based on specialty, scope of clinical practice, and/or business purpose for access. The majority of staff, post graduate students, and medical students met that requirement. However, because some medical schools do not conclude by June 15 and the UC San Diego Fiscal Year begins on July 1, some medical residents or fellows may have only one to two days for orientation and training before starting to treat patients. Due to the compressed timeframe, Epic access was granted prior to training being completed in some cases, creating some risk that patient health records could be incomplete. Physicians who do not have an opportunity to attend system training could also be less satisfied with system performance.

Physicians are hired by the School of Medicine departments, and the on-boarding processes vary by department. We were advised that not all departments enforce the Epic system training requirement. In those cases, new physicians may arrive to treat scheduled patients without completing system training. Lack of Epic system training could result in user dissatisfaction with the system and incomplete information in patient records.

Access Monitoring

University policy states that access management control objectives should include a periodic review of user system activity and access rights. The Health Sciences Compliance and Privacy Program has implemented the Fair Warning Program, which monitors compliance with patient privacy regulations through the use of a “Break the Glass” application. This Program is a critical component of an overall user access monitoring effort. However, routine periodic review of user access to the system development and/or production environments is also important and was not

consistently performed due to competing work priorities. To facilitate a periodic user review, the Epic User Auditing Guide provides some basic auditing techniques to assist with monitoring user access.

Management Corrective Actions:

The CA Support Team will:

1. Pilot a procedure using a monthly worksheet of new hires received by IS to identify new physicians and contact Departments to schedule Epic training as part of the on-boarding process.

2. Identify the standard data fields required to grant access to the EHR. Specific consideration will be given to users without an employment relationship to the University.

3. Develop Epic user access request procedures that provide guidance to departments, and identify all required data elements.

4. Develop a routine Epic user monitoring plan focused on high risk users or activities.

B. Duplicate and Generic User Accounts

Duplicate and generic user accounts increased the risk of unauthorized system access and not-compliance with HIPAA Privacy standards.

Per University policy, the creation of a unique identification for users with authorized access is an important control objective. Because systems record user activity based on the user account identification number (ID), and not the individual username, user accounts should always correspond to a unique individual. Also, each user should be assigned only one account.

AMAS used a composed field (Last Name + First Name + Last 4 digits of the Social Security number + Date of Birth) to identify duplicate user accounts. Using that methodology, 43 duplicate users were identified. Those users were linked to 99 individual user accounts. We were advised that a number of those accounts were created by the Epic Team for system test purposes.

While analyzing user account data, we also identified 66 active generic accounts (out of 100 user accounts in numeric format) with user names such as "OO, OO;" "Care Anywhere;" and "Inpatient Physician". A number of those accounts were not linked to a security template or role, and others were associated with various roles and security levels. Generic accounts are typically created with the intent of providing access to more than one user via a generic password. In the absence of a valid

business purpose, active generic accounts increase the risk of intentional or unintentional unauthorized access to PHI.

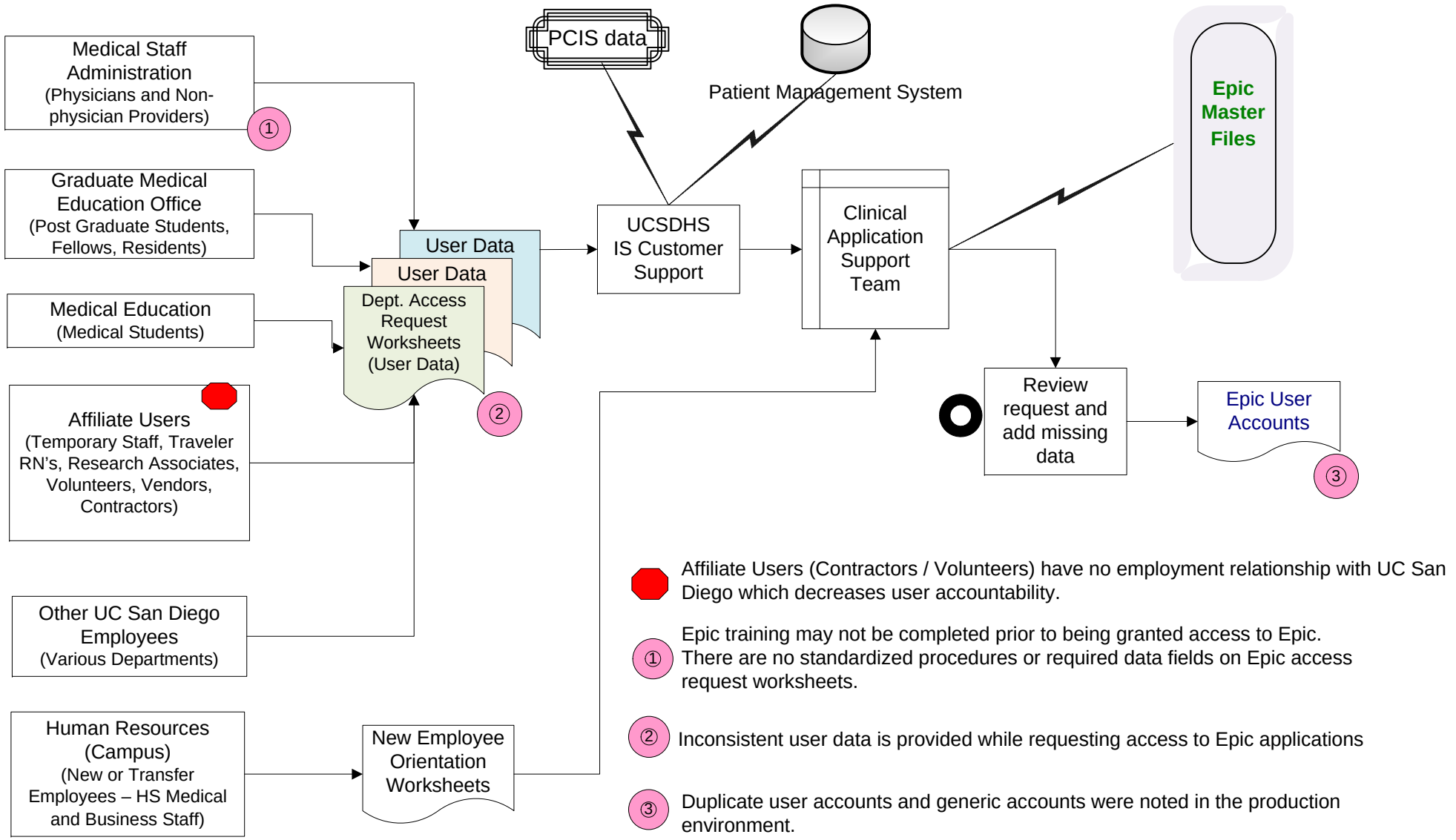
Management Corrective Actions:

The CA Support Team will:

1. Examine the duplicate and generic user accounts in the current user list and retain only the accounts with a valid business purpose.

2. Develop a standard naming convention when establishing generic accounts for completing Epic system tests.

Epic Electronic Health Records: User Access Management
Audit & Management Advisory Services Project #2013-13
Epic User Access Request and Review Processes



Affiliate Users (Contractors / Volunteers) have no employment relationship with UC San Diego which decreases user accountability.

① Epic training may not be completed prior to being granted access to Epic. There are no standardized procedures or required data fields on Epic access request worksheets.

② Inconsistent user data is provided while requesting access to Epic applications

③ Duplicate user accounts and generic accounts were noted in the production environment.

The process for identifying and correcting missing or incomplete data is a strong internal control.

Attachment A