UNIVERSITY OF CALIFORNIA, SAN FRANCISCO
AUDIT AND ADVISORY SERVICES

Medical Center
Medical Staff Service Office
ECHO System Review
Project #15-018

January 2015

University of California
San Francisco

UCSF

Audit and Advisory Services

January 14, 2015

KOSAL BO
Director
Medical Staff Service Office

SUBJECT: Medical Staff Service Office (MSSO) ECHO System Review

As a planned internal audit for Fiscal Year 2015, UCSF Audit and Advisory Services ("AAS") conducted a review of Medical Staff Service Office (MSSO) ECHO System. This review was performed in November 2014. Our services were performed in accordance with the applicable International Standards for the Professional Practice of Internal Auditing as prescribed by the Institute of Internal Auditors (the "IIA Standards"). Our preliminary draft report was provided to management of MSSO in December 2014.

Management provided us with their final comments and responses to our findings and recommendations in January 2015. The observations and corrective actions have been discussed and agreed upon with department management and it is management's responsibility to implement the corrective actions stated in the report. In accordance with the University of California audit policy, AAS will periodically follow up to confirm that the agreed upon management corrective actions are completed within the dates specified in the final report.

This report is intended solely for the information and internal use of UCSF management and the Ethics, Compliance and Audit Board, and is not intended to be and should not be used by any other person or entity.

Sincerely,

Irene McGlynn

Irene McGlynn
Director

cc: Chief Medical Officer Adler
Director Collins
Dr Cucina. M.D.
Director Ridley
Director Smith

Medical Staff Service Office
ECHO System Review
Project #15-018

MANAGEMENT SUMMARY

As a planned audit for Fiscal Year 2014-2015, Audit and Advisory Services completed a review of the ECHO system (ECHO) which is co-managed by the Medical Staff Service Office (MSSO), Referral Services, and Graduate Medical Education.

The purpose of the review was to assess the internal controls in place for maintaining accurate provider information within ECHO and its integration with other systems.

Procedures performed as part of the review included interviews with departmental management and personnel; review of relevant policies and procedures; assessment of ECHO data; and integrity testing for a sample of provider information in APeX.

Based on the work performed, opportunities for improvement exist in the management of information for off-boarding providers and compliance with Office of Inspector General (OIG) requirements for sanction monitoring. Additionally, ECHO password enforcement, security controls, and shared accounts need to comply with University requirements. The integrity of uploaded ECHO provider information in APeX requires additional process to ensure accuracy. Finally, MSSO should evaluate its organizational structure and processes for credentialing and privileging to determine whether it will meet the future demands of the UCSF Health system.

Additional information regarding the observations and associated management corrective action plans is detailed in the body of the report.

I. BACKGROUND

As a planned audit for Fiscal Year 2014-2015, Audit and Advisory Services completed a review of the ECHO system (ECHO) which is co-managed by the Medical Staff Service Office (MSSO), Referral Services, and Graduate Medical Education. ECHO is a web-based software from the HealthLine Systems Inc., designed for effective management of credentialing and privileging processes for medical staff.[1] At UCSF, ECHO was implemented in 2011 prior to the APeX roll-out in 2012.

The provider information in ECHO is interfaced with several clinical applications, including: APeX, Sunquest LIS (Clinical Lab system), IDXRad (Radiology), BREAST-Mammo (Mammography), CoPath (Pathology and Clinical lab medicine), Mossaiq (Radiation Oncology), NCentaurus (Call Center), and OZ Tech Labsys (lab results reporting). Because of its integration with so many systems, it is important that the provider information in ECHO is accurate.

ECHO was initially deployed to manage the credentialing and privileging processes for UCSF medical staff. In order to accommodate UCSF's increasing operational needs[2], ECHO is now utilized to manage additional types of providers. The table below illustrates examples of different groups of providers and allied professional data maintained with in ECHO:

Type of Accounts	Number of Active Accounts[3]	Credentialing and/ or Privileging	Managed By	Description
Medical Staff	2,694	Credentialing and Privileging	MSSO	• UCSF medical staff who practice at UCSF locations • Providers at Langley Porter Psychiatric Hospital and Clinics • UCSF medical staff who practice at non-UCSF locations (including Queen of Valley, Salinas Country Pediatrics, and Santa Rosa Clinic) • Courtesy or volunteer providers • Clinical associates from other medical groups (including One Medical Group, Golden Gate Pediatrics/OBGYN, Tamalpais Pediatrics) • Non-UCSF medical staff from affiliated hospitals (including Benioff Children's Hospital Oakland)

[1] Credentialing is an examination and review of the credentials of individuals meeting a set of educational or occupational criteria and therefore being licensed in their field. Privileging is the permission granted to a medical staff member or Advanced Health Practitioner (AHP) to render specific patient services.
[2] The operational needs have changed due to increased clinical integration and affiliations as part of the UCSF Health Systems.
[3] Based on data extracted from ECHO on September 18, 2014.

Type of Accounts	Number of Active Accounts[3]	Credentialing and/ or Privileging	Managed By	Description
Auxiliary	415	Neither	MSSO	• UCSF staff who have no regulatory credential requirements, but need to obtain UCSF Provider IDs in order to access patient care data in clinical applications (e.g. Audiologists, Occupational Therapists, etc.)
Credential Verification Office (CVO)	47[4]	Credentialing	MSSO	• Dental professionals in the UCSF School of Dentistry
Residents	1,585	Privileging	Graduate Medical Education	• UCSF residents
Referring Providers	45,448	Neither	Referring Services	• Non-UCSF medical personnel who may refer patients to UCSF

II. AUDIT PURPOSE AND SCOPE

The purpose of the review was to assess the internal controls in place for maintaining accurate provider information within ECHO and integrating ECHO with other systems. The scope of the review covered data contained in ECHO. The procedures performed to conduct the review included the following:

- Interviewed MSSO and Information Technology (IT) management and personnel to gain an understanding of the process for administering ECHO and managing provider data;
- Compared active providers in ECHO against APeX and Individual Identifier System database (IID) to identify separated providers who still had active accounts;
- Assessed existing processes for deactivating accounts for providers in ECHO;
- Reviewed re-appointment of medical staff to validate if this had occurred prior to re-appointment due date;
- Interviewed Referring Services personnel to gain an understanding of processes for managing referring providers' information;
- Assessed existing processes for updating contact information for referring providers to ensure the validity of the information;
- Reviewed a sample of data elements for provider information in ECHO and APeX for consistency and accuracy;
- Reviewed ECHO user accounts to ensure that access to ECHO is granted to appropriate personnel and access level;
- Interviewed IT personnel to gain an understanding of security of data in ECHO during transmission; and,
- Reviewed ECHO password and account lockout settings to ensure compliance with University requirements.

[4] CVO accounts do not include current dental professional applications in process.

Since work performed was limited to the specific procedures identified above, this report is not intended to, nor can it be relied upon to provide an assessment of the effectiveness of controls beyond those areas and systems specifically reviewed. Fieldwork was completed in October 2014.

III. CONCLUSION

Based on the work performed, opportunities for improvement exist in timely deactivation of ECHO accounts for providers who no longer work or practice at UCSF and compliance with Office of Inspector General (OIG) requirements for sanction monitoring to ensure that provider data in ECHO is accurately maintained.

Additionally, ECHO password enforcement, security controls, and shared accounts need to comply with University requirements to ensure that provider data in ECHO are securely managed. The integrity and accuracy of data in APeX require additional controls to ensure that provider data in ECHO are accurately uploaded to APeX.

Further, an assessment needs to occur in determining whether the existing organizational structure for credentialing and privileging will meet the future needs of the UCSF Health system and comply with regulatory standards for ongoing professional practice evaluation for medical staff.

Detailed information on these observations and associated management corrective action plans are outlined in the table below.

A. Medical Staff Service Office

No.	Observations	Risks/Effect	Proposed MCA
A.1	**<u>Credentialing and Privileging</u>** ***The existing process for credentialing and privileging clinical associates and affiliates does not fully meet Joint Commission Standards.*** The growth in clinical integrations and affiliation arrangements by UCSF has resulted in MSSO acting as the credentialing and privileging office for a number of medical practices.[5] However, this has created compliance issues in privileging some types of providers as MSSO is not able to meet the Ongoing Professional Practice Evaluation requirement in accordance with the Joint Commission Medical Staff Standard MS 08.01.03. For example, MSSO is relying on outside information to assess a provider's ongoing competency to perform privileges that are granted because there is no UCSF-specific performance data for Department Chairs to review. Such providers include clinical associates (e.g. providers in One Medical Group) and UCSF providers practicing off-site. It was noted that efforts are underway to establish processes for these types of arrangements that are expected to address the compliance concerns. Until that occurs, UCSF will be non-compliant with Joint Commission Standards. Additionally, due to the potential for other future contracting arrangements, the existing structure of combined credentialing and privileging may not be sustainable. A typical model at other institutions (e.g. UCLA, Kaiser) is to have a separate credentialing verification office (CVO) that differentiates the privileging aspects.	The process for credentialing and privileging non-UCSF providers may create compliance concerns.	By June 30, 2015, MSSO will complete an assessment of existing criteria and structure for credentialing and privileging providers for clinical integration purposes. Based on the assessment results, MSSO will implement the structure and develop written procedures suitable for each type of provider.
A.2	**<u>Provider Account Management</u>** ***Accounts of providers that have separated from UCSF are not deactivated timely*.** MSSO is dependent on departments to notify them of changes in provider's status. Review and comparison of active providers in ECHO to IID identified that the following number of providers had separated from the University but were still active in ECHO:	Failure to deactivate accounts of providers who no longer have any business reasons for access can	1. By March 31, 2015, MSSO will establish and implement procedures for reviewing active provider accounts

[5] These practices include One Medical Group, Golden Gate Pediatrics/OBGYN; Tamalpais Pediatrics.

No.	Observations	Risks/Effect	Proposed MCA
	- 36 Auxiliary -- As there is no re-credentialing process for Auxiliary providers, the account will stay active indefinitely if no action is taken. - 70 Attending and 17 Advanced Health Practitioners -- As re-credentialing occurs every two years (three years for DDSs), the risk that active status will remain is up to three years. Additionally, there are inconsistencies in the process for handling off-boarding providers. Certain providers may need to remain as active providers for billing purposes in APeX for a period of time; however, certain privileges (e.g. accepting new appointments, prescribing, etc.) should be removed immediately. University Policy IS-3 stipulates that user access must be revoked upon termination, or when job duties no longer require a legitimate business reason for access (IS-3§III.C.1.a).	lead to inaccuracies in other interfaced applications and may create compliance issues.	in ECHO by comparing to the IID data feed on a quarterly basis. 2. By May 31, 2015, MSSO, in partnership with the APeX IT team, will establish and implement procedures for handling off-boarding of providers.

B. Referral Services

No.	Observations	Risks/Effect	Proposed MCA
B.1	**<u>Deactivating Referring Providers</u>** ***There is no on-going process for deactivating ECHO accounts for dormant referring providers.*** There are currently about 45,000 active referring providers in ECHO. Annually, Referral Services sends a fax to all referring providers to verify the accuracy and validity of contact information. The response rate by referring providers is approximately 70%. However, providers who do not respond are not deactivated, and consequently are left in APeX indefinitely. This increases the risk of users selecting and sending patient health information correspondence to incorrect addresses or faxes, resulting in a potential breach of patient health information under Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations.	Outdated or invalid contact information for referring providers will increase the risks of privacy breaches.	By March 31, 2015**,** Referral Services will develop and implement a process for identifying and deactivating providers who do not confirm their contact information.

No.	Observations	Risks/Effect	Proposed MCA
B.2	**<u>Sanction Monitoring for Referring Providers</u>** ***On-going sanction monitoring practice for referring providers is limited only for revoked or suspended MD licenses in California.*** Referring Services receives notifications from the California Medical Board for revoked or suspended licenses and deactivates provider accounts based on this. However, there is no other on-going sanction monitoring or comparison of referring providers against OIG exclusion list to discern any matched providers. Under sections 1128 and 1156 of the Social Security Act, OIG requires that no Federal health care program payment may be made for any items or services furnished (1) by an excluded person or (2) at the medical direction or on the prescription of an excluded person.[6]	Claiming reimbursements for patients in Federal programs (Medicare and Medicaid) for services based on medical directions and orders that are referred by excluded providers or providers whose licenses are suspended/ revoked is in violation of regulatory requirements.	By March 31, 2015, Referral Services will consult with Compliance, Campus Office of Legal Affairs and Office of General Counsel on the sanction monitoring requirements for referring providers and revise its monitoring process as necessary.

C. ECHO Security and User Account Management

No.	Observations	Risks/Effect	Proposed MCA
C.1	**<u>Enforcement of Password Rules</u>** ***University password requirements are not met.*** Current password configuration for ECHO does not comply with University password requirements in terms of complexity. The minimum password length is set at four	Weak password controls increase the risks of University systems being compromised by	At the close of the audit, a change was made to enforce password rules to meet University requirements.

[6] According to OIG's Special Advisory Bulletin on the Effect of Exclusion from Participation in Federal Health Care Programs, any items and services furnished at the medical direction or on the prescription of an excluded person are not payable when the person furnishing the items or services either knows or should know of the exclusion. An excluded provider may refer a patient to a non-excluded provider if the excluded provider does not furnish, order, or prescribe any services for the referred patient, and the non-excluded provider treats the patient and independently bills Federal health care programs for the items or services that he or she provides.

No.	Observations	Risks/Effect	Proposed MCA
	characters and password complexity is not required. UCSF Unified Password Standards defines the minimal requirements of passwords, including minimum password length of seven characters and password complexity.[7]	making it easier for unauthorized individuals to gain access through hacking or guessing of passwords.	No further action required.
C.2	**SSL Certificate** ***Secured Socket Layer (SSL) digital certificate is not used for ECHO.*** Although access to ECHO is limited through intranet or VPN, SSL[8] is not being used for ECHO. Therefore, confidential information, including passwords and Social Security Numbers (SSNs), is not encrypted during transmission and may be susceptible to compromise. IS-3 stipulates suitably strong encryption to be employed when passwords are transmitted over a network as network traffic may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise (IS-3§IV.B).	Use of unencrypted network protocol increases the risk that sensitive information is sniffed and compromised during the data transmission.	By March 31, 2015, MSSO, in conjunction with IT Business/Clinical Applications, will implement SSL for ECHO.
C.3	**Shared Accounts** ***Shared accounts are used to access ECHO contrary to University Policy.*** A review of user accounts and interviews with IT Business/Clinical Applications personnel identified five "read-only" accounts which are shared by a group of users. Although users of the shared accounts are not able to change data in ECHO, University policy prohibits the use of shared accounts. Additionally, shared accounts are used by Departments within UCMe, a subsystem/portal of ECHO used for credential requests. Information entered by departments in UCMe includes name, date of birth (DOB), SSNs and government-issued identification (e.g. driver's license).	Use of shared accounts compromises accountability and precludes the ability to identify personnel responsible for operations/activities using the accounts.	1. By February 28, 2015, MSSO, in conjunction with IT Business/Clinical Applications, will assess all shared accounts to determine whether shared access is justified. If shared accounts are determined as necessary, a formal exception approval

[7] Unified UCSF Enterprise Password Standard

[8] Secure Sockets Layer (SSL) is a protocol that uses encryption to ensure the secure transfer of data over the Internet.

No.	Observations	Risks/Effect	Proposed MCA
	IS-3 stipulates that accounts/passwords should never be shared with other individuals unless specifically approved and documented as an exception (IS-3§III.C.3.b).		will be obtained from IT Security. The business reasons and name of personnel using the shared accounts will be documented for each account. 2. By February 28, 2015, MSSO, in conjunction with IT Business/Clinical Applications, will create individual accounts for UCMe.
C.4	<u>**Display of Social Security Number (SSN)**</u> ***Providers' SSNs are displayed for all ECHO users.*** A review of ECHO identified that SSNs for providers are displayed for all users. According to MSSO and IT Business/Clinical Applications, ECHO users who need to edit records use SSNs to verify providers; however, read-only accounts (four users and six shared accounts) do not need to view SSNs.	Displaying SSNs to users who do not have a business reason to view SSNs increases the risks of unauthorized use.	During the course of the audit, a change was made to mask SSNs for read-only users. No further action required.

D. ECHO Data in APeX

No.	Observations	Risks/Effect	Proposed MCA
D.1	**<u>Discrepancies in APeX</u>** ***Data from ECHO is not always accurately uploaded to APeX.*** Comparison of provider information in APeX and ECHO identified the following discrepancies: • 20 records - Status is active in APeX for providers who have inactive status in ECHO • 43 records – Status is no value (=Null) in APeX for providers who have active status in ECHO[9] • 3 records - Providers have privileges in APeX when they should not • 2 records - Provider ID is assigned to a different provider in APeX • 3 records - Provider has two active APeX accounts • 1 record - External provider is uploaded as internal provider in APeX • 5 records - Specialty is not assigned in APeX for providers who have specialties in ECHO • 20 records - Provider ID format is incorrect in APeX	Inaccurate provider information increases the risks that invalid provider information is utilized for patient care or billing and also reduce the reliance on the integrity of the data.	IT APeX team has performed an analysis to investigate the discrepancies identified and data refresh to correct provider information in APeX. Results of the investigation showed that root causes for some of the discrepancies were inconclusive. By April 30, 2015, IT APeX team will develop a process for quarterly review to ensure accuracy of ECHO data upload into APeX.

[9] IT APeX team confirmed that APeX accounts are considered as active if there is no value in status; therefore, the risk is low.