UNIVERSITY OF CALIFORNIA, SAN FRANCISCO
AUDIT SERVICES

UCSF Medical Center
EHR – Monitoring Access to Patient Records
Project #14-038

June 2014

Fieldwork Performed by:

Sugako Amasaki, Principal Auditor

Reviewed by:

Tom Poon, Senior Associate Director

Approved by:

Zuleikha Shakoor, Senior Associate Director

EHR – Monitoring Access to Patient Records
Project #14-038

MANAGEMENT SUMMARY

As a planned audit for Fiscal Year 2014, Audit Services conducted a review of the effectiveness of the practices and procedures established for monitoring access to patient records within UCSF's Electronic Health Records (EHR) system, the Advanced Patient-Center Excellence (APeX) system, for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations.

The successful implementation of APeX system has tremendously improved availability of patient records. At the same time, the complexities of the operations make it difficult to limit access to the minimum information necessary to do a job as some employees' effectiveness could be significantly inhibited without seamless access. As a result, the increased availability and accessibility of patient records created greater risks of unauthorized access to patient records.

The HIPAA defines Security and Privacy requirements for mechanisms needed to monitor access to patient records, including:

- Implementation of hardware, software, and procedural mechanisms that record and examine activities in information systems that contain or use electronic protected health information.
- Implementation of procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Procedures performed as part of this review included interviews with personnel in the Privacy Office, the Concierge Program, and the UCSF Information Technology; reviews of relevant documents; and a walk through of the existing process to determine the adequacy of procedures in place for monitoring access.

Based on work performed, the existing procedures for monitoring of access to patient records is limited to a monthly audit performed by the Concierge Program and the Privacy Office. The effectiveness of this monitoring is hindered due to the manual labor intensive process and the partial information available to accurately determine whether only appropriate personnel had accessed the patient records. While the Medical Center has implemented some measures for monitoring access to patient records, a more comprehensive monitoring program is needed to ensure compliance with HIPAA requirements are fully met, accountabilities are defined and confidentiality of patients' information is adequately protected. It was noted that the absence of an effective automated monitoring tool has restricted implementation of a robust and effective monitoring program.

Additionally, effectiveness of APeX's Break-The-Glass (BTG) functionality could be enhanced to increase monitoring efforts, rather than the current designed use which only serves as a warning alert to the user of their responsibilities and the appropriateness of their access.

Additional information regarding the observations and management corrective actions is detailed in the body of the report.

EHR – Monitoring Access to Patient Records
Project #14-038

TABLE OF CONTENTS

I. BACKGROUND

As a planned audit for Fiscal Year 2014, Audit Services completed a review of the effectiveness of Medical Center's practices for monitoring access to patient records. The review covered patient records stored within the APeX system.

The advent and wide use of electronic health records (EHR) has tremendously improved operations; at the same time, the increased availability has created risks of unauthorized access to patient records. UCSF's EHR system, APeX, was implemented in 2012, and generates audit logs of all access to patient records. Additionally, the APeX has an embedded functionality, "Break-The-Glass" (BTG), which informs users that they are attempting to access restricted records and requires entering a reason for the access.

UCSF Medical Center policy requires that upon hire, all the Medical Center employees, including contract and temporary employees and volunteers, read and sign the "Privacy Confidentiality Statement" which includes a clause for agreeing that access, use or disclosure of confidential information is only in the performance of University duties.[1] [2] A similar process is employed in the schools for students and through the Medical Staff Office for attending physicians.

The regulations governing the confidentiality and protection of patient health records are contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which defines the Security and Privacy requirements for mechanisms needed to monitor access to patient records, including:

- Implementation of hardware, software, and procedural mechanisms that record and examine activities in information systems that contain or use electronic protected health information.[3]
- Implementation of procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.[4]

Compliance with these HIPAA Privacy and Security requirements is also necessary in order to be considered as 'eligible' to receive incentives under Meaningful Use.[5] In recent years there has been increased focus by the media and regulatory agencies on the protection of patient health information. Failure to have appropriate systems and processes in place to protect the confidentiality of patient medical records can result in fines and penalties should breaches occur. Additionally, it could lead to patients' dissatisfaction and loss of confidence in the institution.

[1] UCFS Medical Center Policy 5.02.01:Confidentiality, Access, Use, and Disclosure of Protected Health Information and Patient Privacy

[2] Statement of Privacy and Confidentiality Laws and University Policy and the Acknowledgement of Responsibility

[3] 45 CFR §164.312(b): Audit controls

[4] 45 CFR §164.308(a)(1)(ii)(D): Security Management Process

[5] Meaningful Use Core Measures require a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implementation of security updates as necessary and correct identified security deficiencies as part of its risk management process.

II. AUDIT PURPOSE AND SCOPE

The objective for this review was to assess the current systems and procedures established for monitoring access to patient medical records within APeX for compliance with HIPAA regulations.

To conduct the review, Audit Services interviewed personnel within the Privacy Office, the Concierge Program, and the UCSF Information Technology (IT) to gain an understanding of existing monitoring practices, including monthly audits and the BTG functionality. We reviewed relevant documents, access records for a sample of patients, and results of monthly audits performed by the Concierge Program, Privacy Office and ITS. Additionally, we contacted other UC Medical Centers to gather information on practices and tools used for monitoring access to patient medical records to identify best practices.

Work performed was limited to the specific procedures stated; this report is therefore not intended to, nor can it be relied upon to provide an assessment of the effectiveness of controls beyond those areas and processes, specifically reviewed. Further, this assessment represents the status of EHR monitoring processes effective as of the date of fieldwork; process modifications subsequent to the completion of this review may result in a different controls environment than what is communicated in this report. Fieldwork was completed in March 2014.

III. CONCLUSION

Based on work performed, the Medical Center has a limited monitoring program in place that does not sufficiently meet HIPAA requirements. The existing monitoring of access to patient records to identify any inappropriate access is performed by Concierge Program and Privacy Office, and is limited to a monthly audit of a small number of patients from a list of inpatients that are UCSF employees or came through the Concierge Program. The review identified the need for a comprehensive proactive monitoring program to detect inappropriate access to patient records and a governance structure that defines the monitoring criteria, sampling methodology for determining the number of records to be reviewed and responsible parties for review and follow-up. Additionally, the absence of data analysis and modeling tools has impeded the Medical Center's ability to implement effective and efficient monitoring practices as reviews of a large amount of access log data cannot occur manually or through limited reporting. Lastly, there is no monitoring of the BTG audit logs to ensure appropriateness of access; rather the Medical Center has deployed BTG as a warning tool only. Additionally, the BTG has an inherent design weakness that does not provide full protection of confidential patient records.

Implementation of automated tools and development of a more comprehensive monitoring program will put the UCSF's program in line with other UC Medical Centers' monitoring programs.

IV. OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

A. Comprehensive Monitoring Program

***A comprehensive program for monitoring inappropriate access to patient records has not been established*.**

UCSF Medical Center has implemented limited processes to monitor access to patient records; however, there is no comprehensive monitoring program with defined criteria on triggers for potential inappropriate access, and frequency of reviews for monitoring inappropriate access to patient records. To this end, a governance structure or a Committee/Workgroup has not been created to assume the responsibility for establishing the program, including the assessment of the risks, compliance requirements, tasks, and accountabilities.

Discussions with the Privacy Officer highlighted that the implementation of an effective and comprehensive monitoring program has been hindered due to the absence of a robust data analysis and modeling tools that will enable an efficient review of the large amounts of audit log data.

Absence of governance and a comprehensive monitoring program can increase the risks of inappropriate accessing of patient records going unnoticed and potential fines and penalties for non-compliance with HIPAA requirements.

B. Break-The-Glass (BTG)

The BTG is a functionality within the Electronic Health Record system that informs the user that the patient record being accessed is restricted, prompts the user to enter a reason to access the patient record, and requires the user to re-authenticate credentials before granting access. The system generates audit logs that can be used to audit the access for appropriateness.

Assessment of the BTG utilized at UCSF identified the following:

1. The BTG controls can be by-passed

The BTG was initially configured to trigger whenever medical records for patients classed “confidential” were accessed. However, due to the impact on operational workflows, a decision was made to limit the BTG to trigger when patient level information is accessed with some exceptions added to the criteria for triggering the BTG.[6] Additionally, the BTG has an inherent design weakness which hinders the ability to monitor complete access of confidential patient records.[7]

[6] If users are in the treatment team, admitting/attending provider, or PCP of the patient or if users break the glass during the prior 7 days, the BTG will not be activated.

[7] Some portions of confidential patient records can be accessed without triggering the BTG, such as registration, appointment, ADT, referral, billing, coding, and scanned documents. Also, APeX Billing/HIM users can access patient records without triggering the BTG if the Hospital Account Maintenance workflow is used.

2. The BTG logs are not being monitored and reviewed.

The BTG activities are logged, however, there is no review performed of the audit logs for determining appropriateness of the reasons for access. Therefore, the BTG is used for 'warning' purposes only and not to the full extent of its capabilities to monitor.

The ability to by-pass the controls diminishes the effectiveness of the protection that the BTG was intended to provide and can result in loss of patients' confidence should any violations occur. Additionally, by not addressing this limitation to be able to fully utilize the BTG functionality as a tool for monitoring access to patient records, unauthorized access could go unnoticed.

C. Concierge Auditing Program

The monthly audit performed by the Concierge Program for identifying inappropriate access is limited, labor intensive, and ineffective.

The Concierge Program has implemented the Salesforce System (Salesforce) to track information on patients who are flagged as "Concierge Patients" or those employed at UCSF. From Salesforce, the Concierge Program generates a report which lists active inpatients and selects a sample of two patients each month. The APeX Security Team generates APeX access reports for the selected two patients during the 24 hour audit period. The Concierge Program manually identifies title/department information for all APeX users on the access reports and determines appropriateness of access based on this information. Any incidences of suspected inappropriate access identified are reported to the Privacy Office for further investigation.

Typically, a large number of APeX users from various departments appear on the access reports, including residents and students[8]; therefore, the Concierge Program staff can only exercise their knowledge and best efforts in determining possible inappropriate access. The Privacy Office does forwards the list of users on the access reports to departments for determination and confirmation on the appropriateness of the access when information on a departmental manager responsible for each user is known or available.

Failure to implement a mechanism to effectively monitor, access to patient records precludes the detection of unauthorized access.

D. Management Corrective Actions

1. By November 30, 2014, the Executive Director APeX Operations will propose to the Care Technology Governance Committee to take on the governance responsibilities for approval and oversight of a comprehensive proactive monitoring program based on the assessed risks for the APeX system.

[8] There are, on average, about 90 APeX users reviewed by the Concierge Program for each patient (based on the average for September, October, and November audits).

2. The Chief Privacy Officer, the Executive Director APeX Operations, and the Information Security Officer will oversee the process to develop a monitoring program dependent on Capital budget approval that includes the following:

    a. By November 30, 2014, APeX Operations Director will oversee:
    - Assess existing monitoring processes to determine the level of monitoring efforts that should be performed.
    - Evaluate automated analytics tools to permit more effective reporting and monitoring of access to patient medical records.
    - Develop an IT technical project plan for the activation of the identified tool.

    b. By February 28, 2015, Chief Privacy Officer will oversee:
    - Define the criteria for triggers for potential inappropriate access, frequency of reviews, and the monitoring and follow-up of inappropriate access.
    - Develop a communication plan to notify user communities of their responsibilities and the new monitoring process.

    c. By February 28, 2015, the APeX Operations Director will oversee:
    - Implementation of the communication plan to notify user communities of their responsibilities and the new monitoring process.
    - Evaluation of the BTG for enhanced capabilities, or link it to the new identified monitoring tool.

*** * * ***