**UNIVERSITY OF CALIFORNIA, SAN FRANCISCO**
**AUDIT AND ADVISORY SERVICES**

# Epic Master Files
# Project #20-051

**July 2020**

University of California
San Francisco

**Audit & Advisory Services**
UCSF Box 0818
1855 Folsom Street
San Francisco, CA 94143
tel: 415.476.3851
fax: 415.476.3326
www.ucsf.edu

July 8, 2020

**HEIDI COLLINS**
Vice President
Clinical Systems

**SUBJECT: Epic Master Files**

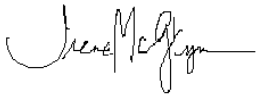
As a planned internal audit for Fiscal Year 2020, Audit and Advisory Services ("A&AS") conducted a review of controls related to access and change management for the selected Epic master files.

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 review was completed and the preliminary draft report was provided to department management in June 2020. Management provided final comments and responses to our observations in July 2020. 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. A&AS 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
Chief Audit Officer
UCSF Audit and Advisory Services

# EXECUTIVE SUMMARY

## I. BACKGROUND

As a planned audit for Fiscal Year 2020, Audit and Advisory Services (A&AS) conducted a review of controls related to access and change management for the following Epic master files:

- User (EMP)
- Security Class (ECL)
- Fee Schedule (FSC)

UCSF's Electronic Health Records (EHR) system, the Advanced Patient-Center Excellence (APeX) system is based on the Epic application. Within the Epic database, data is separated into master files that can be accessed by different activities and transactions. Epic's master files are tables that store records and items related to a particular function or type of entity (such as users, patients, providers, medications, procedures, and fees).

There are two different ways for making changes in the Epic master files in the production environment:

1. Direct changes – There are four data elements (items)[1] in the EMP master file that limited users can make direct changes to the production environment as required for performing assigned tasks. Other data elements in the EMP master file and all records in the ECL and FSC master files cannot be directly changed by users.
2. Changes made through a data courier tool[2] - Only limited and approved personnel are authorized to use a data courier tool (data courier movers), and there are procedures ("UCSF Data Courier Change Management Policies and Procedures") and workflows in ServiceNow established for documenting changes to the production environment.

Some records stored in master files are critical, as they control and manage key components for running the Epic application and impact various operations and transactions (such as user access/security and fees for charges). Therefore, an adequate control environment for access and change management to ensure that only approved changes are made in the master files by authorized personnel is crucial for preventing unauthorized access/changes in the Epic application.

## II. AUDIT PURPOSE AND SCOPE

The purpose of this review was to validate that appropriate controls for access provisioning, de-provisioning, periodic reviews, and change management are in place for selected Epic master files.

The scope of the review covered the following three Epic master files as samples:

[1] 4 items: "Provider ID", "User Account status", "login blocked category", and "In Basket classification"
[2] Data Courier is an Epic tool used to transfer data, such as records or category list values, from one Epic environment to another. After testing in the changes in non-production environment, the Data Courier tool can be used to move those records onward to the production environment.

- User (EMP) – User records define what features are available to a person in Epic and the appearance of Hyperspace[3] for that person. User records are shared across applications, so these records include many settings. A person needs a user record to be able to log in to Hyperspace.
- Security Class (ECL) – Security class records define whether a group of users can access certain activities and perform certain actions in the system. These records are used to restrict or increase system access based on the needs for a given group of users.
- Fee Schedule (FSC) - Fee schedule records define the dollar amounts for procedure, medication, or diagnosis related group codes. Revenue applications use fee schedules to track prices, reimbursement amounts, discount amounts, and more.

Procedures performed as part of the review included interviewing personnel within Clinical Systems and Information Technology (IT), reviewing users who can make changes, and performing sample testing for periodic reviews of users and changes made in the master files. For more detailed steps, please refer to Appendix A.

Work performed was limited to the specific activities and procedures described above. As such, this report is not intended to, nor can it be relied upon to provide an assessment of compliance beyond those areas specifically reviewed. Fieldwork was completed in June 2020.

## III. SUMMARY

Based on work performed, it was noted that appropriate controls appear to be in place for ensuring that only approved changes are made in the Epic master files by authorized personnel.

Opportunities for improvement exist in the areas of appropriate approval and testing in the change management practice.

The specific observation from this review is listed below.

1. Appropriate approval and evidence of adequate testing were not always obtained or documented prior to migration to the production environment.

[3] Hyperspace is the Graphical User Interface for Epic (the view to the end user).

## IV. OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

| No. | Observation | Risk/Effect | Recommendation | MCA |
|---|---|---|---|---|
| 1 | ***Appropriate approval and evidence of adequate testing were not always obtained or documented prior to migration to the production environment.***<br><br>Changes are moved to the production environment by authorized data courier movers. Review of a risk based judgmental sample of 50 changes in the master files (EMP, ECL, and FSC) that were moved into the production environment between January 1, 2020 and April 30, 2020 identified the following:<br>• Change Advisory Board (CAB) approval was not obtained (for changes that should have the CAB approval) – 4 cases<br>• There was no evidence of analyst testing performed – 2 cases<br>• User acceptance testing (UAT) was not performed – 1 case<br>• Sufficient UAT information was not documented (such as date performed, identity of the user who validated the test, and results) – 11 cases<br><br>Clinical Systems team has taken various actions to continuously educate users on the requirements for data courier change management processes, including:<br>1. Developing and implementing the "UCSF Data Courier Change Management Strategy and Procedures" that define requirements for CAB approval and testing<br>2. Performing a quarterly audit for a sample of changes and educating users individually<br>3. Developing a training material for "Apex Data Courier Change Management Process" | The absence of adequate approval and/or testing could lead to inappropriate changes being released into the production environment. | Sufficient approval and testing information should be documented for changes to ensure that appropriate approval and testing processes were completed prior to migration to the production environment. | a) The following ServiceNow tickets will be focused and reviewed as part of the quarterly audits:<br>• CAB approval was exempted.<br>• Sufficient testing information was not documented.<br><br>**Responsible Party**: Clinical Systems management<br>**Target Completion Date**: November 30, 2020<br><br>b) Annual training for data courier change management will be provided to new hires and existing users who make changes through LMS.<br><br>**Responsible Party**: Clinical Systems management<br>**Target Completion Date**: November 30, 2020 |

***APPENDIX A***

To conduct our review the following procedures were performed for the areas in scope:

- Reviewed relevant UCSF procedures to gain an understanding on requirements for access management and change management;
- Interviewed key department personnel within Clinical Systems and Information Technology (IT) to gain an understanding on the processes for access and change management for the Epic master files;
- Reviewed a list of active user accounts to verify that accounts belong to separated personnel are removed in a timely manner;
- Reviewed the process for performing periodic reviews to ensure that access is adequate;
- Reviewed a sample of changes made in the Epic master files to validate that established change management procedures are followed; and,
- Assessed appropriateness of access and change management practice in place.