University of California
San Francisco

UCSF

Audit and Advisory Services

June 21, 2017

Deborah Yano-Fong
Chief Privacy Officer
Privacy Office

SUBJECT: **Electronic Health Record (EHR) Monitoring Access to Patient
Records – Follow-Up Review
Audit and Advisory Services Project #17-054**

Audit and Advisory Services (A&AS) performed a follow-up review of the process
of monitoring access to patient records. The objective of the review was to
validate that actions implemented for the "Electronic Health Records Monitoring
Access to Patient Records Review" (audit report dated June 2014) are sufficient
for protecting patient privacy.

To complete the review, the new systems and processes implemented for
monitoring access to patient records were examined through interviews,
walkthroughs, and reviews of documentation. Fieldwork was completed in June
2017.

The scope of this review was limited to the systems and processes for monitoring
access to patient medical records within APeX associated with the risks identified
in the audit report dated June 2014, and as such, we can make no assertions
about outside the stated process reviewed, nor can our work be relied upon to
identify all instances of potential irregularities, errors, and control weaknesses
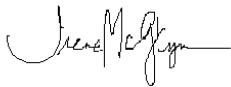that may occur in areas not covered in this review.

As part of this follow-up review, we discussed with UCSF Privacy Office ("Privacy
Office") to gain an understanding of the Privacy Office's implementation of Iatric's
Security Audit Manager (SAM) solution in conjunction with CynergisTek's
Managed Privacy Monitoring Services (MPMS) that began in May 2015. The
purpose of the implementation was to establish an effective EHR access auditing
and monitoring plan, proactive audit-related processes, and effective auditing
and monitoring of user activities. A phased approach for using SAM and MPMS
at UCSF was detailed as part of the plan, including implementation of a gradual
escalation process and essential processes, a recommendation plan for alerts
and reports to include frequency and distribution, and a normalization process
approach for behavioral modeling to support the identity theft and fraud detection
program.

Currently, CynergisTek runs reports based on criteria from the Privacy Office (and Concierge Services for the "Concierge Audit Reports") or ad-hoc requests, analyzes results, and creates incident tracking records (ITRs) in Iatric's SAM if there are any potential inappropriate accesses that require further reviews by the Privacy Office (and Concierge Services as needed). The activity logs, associated reports and status of each ITR are documented and retained in Iatric's SAM. CynergisTek also provides monthly and quarterly reports to the Privacy Office that include summary and analytical information (such as ITR incident status and trend analysis).

Based on procedures performed, it was noted that Privacy Office has made numerous improvement in the systems and processes in addressing risks identified in the audit report dated June 2014. However, we understand that the initial project plan developed by the vendor (CynergisTek) that includes scope, frequency, and timeline was not supported with sufficient feasibility analysis, including resources needed for the audits, or usability of various CynergisTek reports, and therefore was not attainable. As a result, Privacy Office, in conjunction with CynergisTek, is in the process of re-assessing the usability of various reports and refining certain reports to maximize the use of CynergisTek's MPMS. We recommend Privacy Office to continue these efforts for improving the monitoring of access to patient records.

We thank you and your staff for all the assistance provided during this review.

Sincerely,

Irene McGlynn
Director
UCSF Audit & Advisory Services