UNIVERSITY OF CALIFORNIA, SAN FRANCISCO
AUDIT AND ADVISORY SERVICES

Student Record Security Review
Project #17-041

May 2017

University of California
San Francisco

UCSF

Audit and Advisory Services

May 15, 2017

ELIZABETH WATKINS
Vice Chancellor, Student Academic Affairs and Dean, Graduate Division

SUSAN MASTERS
Associate Dean for Curriculum, School of Medicine

SUBJECT: Student Record Security Review

Audit and Advisory Services ("A&AS") conducted a review on student record focusing on Office of Registrar and School of Medicine to determine compliance with the Family Educational Rights and Privacy Act (FERPA) and University policy. 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 management in March 2017. Management provided us with their final comments and responses to our observations in May 2017. 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, 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
Director
UCSF Audit and Advisory Services

EXECUTIVE SUMMARY

I. BACKGROUND

As a planned audit for Fiscal Year 2017, Audit and Advisory Services completed a review of student record security to assess the practices for safeguarding students' privacy, including system access to education records, and to determine our compliance with the Family Educational Rights and Privacy Act (FERPA)[1] and University of California (UC) policies[2] for the Office of Registrar (OOR) and School of Medicine (SOM). OOR maintains aspects of educational records within the Student Information System (SIS) and provides the following services: ordering transcripts, obtaining diplomas, verifying degrees, changing names, scheduling classrooms, paying fees, and others. SOM also maintains education records in MedSIS, a separate student record system, specific to the student's school performance, onboarding administrative documents and data for use in program evaluation and educational research.

FERPA is a federal law that protects the privacy of student education records and applies to matriculated students and former students. It requires educational institutions to obtain written consent of the student prior to disclosing personally identifiable information from education records to third parties, with several exceptions, including non-opt out directory information, in the case of safety emergency situations, and to state/local authorized officials.

There are currently two separate, ongoing initiatives that will impact student record systems. The Committee on Educational Technology (CET) is tasked with identifying all applications and systems related to students and building a risk profile, which will be used to identify systems with restricted data requiring a more detailed, full IT security risk assessment. Another initiative is the evaluation by the Schools of Dentistry, Nursing, and Pharmacy for new student information systems modeled after MedSIS.

While these changes are underway, we recommend any findings in this report to be shared with the schools for leveraging expected controls in place for safeguarding student education records.

II. AUDIT PURPOSE AND SCOPE

The purpose of this review was to assess UCSF procedures for effectiveness of controls in place to comply with FERPA and UC policies and to determine the appropriateness of system access for student record systems. Interviews were held with personnel from OOR, SOM, School of Dentistry, School of Nursing, Global Health, Graduate Division, and Alumni Relations. As OOR's SIS is the central point for student records and SOM's MedSIS is being evaluated for extension to additional Schools, a more detailed review was conducted for them.

The scope of the review included analyses of student record requests and user accounts for OOR and SOM for the period June 2015 to July 2016.

[1] FERPA (34 CFR Part 99) defines educational records as records that contain information directly related to a student and which are maintained by an educational agency or institution.

[2] UC Policies Applying to Campus Activities, Organizations and Students (PACAOS): 110- student grievance procedures and 130.00-disclosure of information from student records; and UC Records Retention Schedule.

Procedures performed as part of the review included interviews of OOR and SOM department personnel to understand processes for handling student record requests, examination of system access controls and training, review of observations from prior FERPA reviews at other UC campuses, identification of FERPA and UC policy requirements regarding student records, and assessment of record requests to determine FERPA compliance.

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 March 2017.

III. SUMMARY

Both OOR and SOM require FERPA training for their respective users who have access to student records. Additionally, the Staff & Faculty section of OOR's website has FERPA related policies, including a summary of key concepts and a detailed training handout. OOR provides students with annual FERPA notification, including instructions on how to opt-out of sharing directory information (e.g. email, address, and phone number) within SIS.

Both departments have recently completed system access reviews to remove access for terminated or transferred employees. In addition, SOM has an online request method for certain types of data requests including system access where user verification of having read the FERPA Privacy Act before the request can be granted, and requires that educational data for research has CHR approval prior to distributing data.

Although FERPA awareness is present, the oversight activities for tracking and monitoring compliance can be improved in the areas of: written procedures on handling and tracking different types of student record requests, training and system access controls. The specific observations for this review are listed below.

A. System Access for SIS and MedSIS

1. Access management procedures for SIS and MedSIS were not sufficiently established to protect student information.
2. MedSIS access review did not sufficiently include key attributes such as reviewing for inactivity or confirming with users for transfers or role changes.

B. FERPA Oversight Activities

1. There is no recordkeeping of FERPA training course completion by staff members.
2. Standard Operating Procedures (SOPs) do not clearly define processes for handling different type of student record requests.
3. An internal process for submitting and evaluating FERPA violation complaints does not exist.
4. Record-keeping requirements are not consistently interpreted or applied.

Further detail on the specific observations along with additional opportunities for improvement can be found in the below section on Observations and Management Corrective Action Plans.

IV. OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

A. System Access for SIS and MedSIS

No.	Observation	Risk/Effect	Recommendation	MCA
1	***Access management procedures for SIS and MedSIS were not sufficiently established to protect student information.*** Review of access management policies and procedures for SIS and MedSIS identified the following: • Account role definition has not been documented for SIS. • Provisioning of roles in a manner that map to application function/role or access level/rules within the application has not been completed for SIS. • Access requests to MedSIS and SIS do not distinguish between requestor and approver other than clarifying if the request is for the requesting user or another individual. • Procedures for periodic review of user access or user access changes have not been established for either SIS or MedSIS. Both OOR and SOM completed an access review for SIS and MedSIS respectively in September 2016. This had not previously been done annually for OOR, but will be moving forward. In March 2014, Accuvant was hired to perform an enterprise information security risk assessment that included education records for Student Academic Affairs and SOM. The assessment noted similar findings as above and they have not	The lack of specific requirements and guidance could result in inconsistent practices that lead to unintended access to sensitive data for terminated employees or employees that no longer need access.	To ensure timely review of accounts and that system access is revoked promptly when users separated from the University or no longer need access, departments should establish formal procedures for provisioning, de-provisioning, and periodic review of user to include: who, when, how, where, what, and by whose authority.	1. OOR will document policies and procedures for access management for SIS. **Responsible Party:** Director Student Info Systems **Implementation Date:** June 30, 2017 2. SOM has drafted and will implement the following procedures: a. Supervisors will be required to submit an online account request form in order to provision access to MedSIS for any new staff. An email confirmation upon request and new account creation will be sent to the supervisor and employee. b. An annual review and renewal of accounts process will be conducted each July. This will include the review and capture of last login for every user and current university affiliation and will be reviewed by the Director,

No.	Observation	Risk/Effect	Recommendation	MCA
	been fully addressed. The lack of current or valid security policies, standards, and procedures were rated as critical risks per the Accuvant report that needed to be addressed as soon as possible.			Student Experience. c. All active users will receive a communication to confirm their continued access and attest to having reviewed the MedSIS User Guide and their continued adherence to protecting data privacy and FERPA. **Responsible Party:** SOM Executive Director of Tech Enhanced Edu **Implementation Date:** July 30, 2017
2	***MedSIS access review did not sufficiently include key attributes such as reviewing for inactivity or confirming with users for transfers or role changes.*** SOM performs MedSIS user account reviews annually by reviewing payroll data for separated employees. The review process did not include the number of days the account had been inactive or verification with users for a business need for access. Specifically, last login date was not captured by MedSIS and 13 out of 185 active accounts did not have user role assigned. Leading practices for account security controls require last login date information in order to have effective account review processes, including monitoring of elevated privilege accounts; when policy or guidelines expect deactivating accounts after a specific period (90 days for restricted or sensitive data); and to assist in incident	The lack of key information, such as last login date, hinders department from applying effective security controls for their account monitoring processes, such as identifying inactivity or inappropriate access at odd hours.	The annual SOM access review should include: adopting threshold and frequency of review for elevated privilege accounts as well as regular user accounts; confirming with users if a business need for access still exists based on inactivity threshold; inactivating accounts that do not have user role assigned; and reviewing accounts with multiple user roles and/or roles with high privilege to reassess validity. Departments should retain evidence of compliance regarding system access control reviews for auditing	SOM implemented capture of the last login date on user accounts for a six-month period during this review. If a 90-day threshold is adopted for elevated accounts or access to sensitive data, this will be a sufficient time period of information captured. However, if a longer period of inactivity threshold is adopted for regular user accounts, this may not be sufficient data. If feasible, it would be beneficial to extend the period to account for the annual assessment of regular user accounts. Requests for new elevated accounts and the de-provisioning of elevated accounts will be initiated and managed by the Director,

No.	Observation	Risk/Effect	Recommendation	MCA
	management.		purposes to demonstrate a pattern of consistent strong compliance and accountability.	Student Experience. **Responsible Party:** SOM Executive Director of Tech Enhanced Edu **Implementation Date:** May 31, 2017

B. FERPA Oversight Activities

No.	Observation	Risk/Effect	Recommendation	MCA
1	***There is no recordkeeping of FERPA training course completion.*** OOR administers periodic in-person FERPA training sessions.[3] There was no formal mechanism to capture staff that had completed training and no requests for evidence of training completion. There are approximately 300 active SIS users from 69 departments and percentage of training compliance status could not be determined. FERPA training reduces the risk of the inappropriate release of student information and tracking would identify compliance performance status.	A lack of FERPA knowledge combined with access to FERPA data could result in the unintentional disclosure of student information and violation of Federal Regulations.	OOR should consider a tracking solution, such as UC Learning Management System, for tracking FERPA training course completion to demonstrate compliance status. For the 300 existing users, OOR should consider a retroactive process of obtaining user attestation and retaining this record for as long as the user is active.	OOR will implement an online training module that will allow tracking of training completion via LMS. Users whose training is not documented on existing login sheets will be required to retake the training. **Responsible Party:** Asst VC-Student Info **Implementation Date:** December 30, 2017
2	***Standard Operating Procedures (SOPs) do not clearly define processes for handling different types of student record requests.*** a. While OOR has a training document to use as a source for operational procedures, it reiterates FERPA requirements and does not cover key procedures to address them, such as:	Undocumented procedures for handling student record requests create inconsistent practices that may result in noncompliance with FERPA and	OOR should develop their SOPs to include as much information as applicable, describing: who, when, how, where, and what to ensure that different type of requests are processed in accordance with FERPA and university requirements.	1. OOR will develop SOP for the different types of student record requests. **Responsible Party:** OOR Asst VC-Student Info **Implementation Date:** September 29, 2017

[3] In 2016, it was held twice, on August 30 and September 7.

No.	Observation	Risk/Effect	Recommendation	MCA
	• Criteria for verification of student identity when inquiries or requests are not in person. • Documentation of the method and criteria for request, timeline for access, and a checklist to ensure the removal of non-education records for student requests to review education records. • Categorization of third party requests, such as when 'opt out' directory information should be excluded or PII will be provided without consent. b. SOM procedures can be enhanced by the following: • Adding a step for the Student Record Analyst (SRA) to determine that documents provided for students requesting to inspect their own records exclude non-education records and recommendation letters that the student has opted-out of viewing. • Tracking student inspection requests, as direct email may not be retained when a new SRA's email is used. This log will demonstrate management of oversight activity. • Implementing review to ensure students' opt-outs are applied for directory information requests.	university policies.	SOM should update their procedures to include quality checks and tracking for student requests.	2. The Student Record Analyst (SRA) will conduct a manual review of all student documents to determine that documents provided for students requesting to inspect their own records exclude non-education records and recommendation letters that the student has opted-out of viewing. All student inspection requests will be logged. SOM does not provide student directory information as part of a student record request as per SOM Policy. **Responsible Party:** SOM Executive Director of Tech Enhanced Edu **Implementation Date:** May 31, 2017
3	***An internal process for submitting and evaluating FERPA violation complaints does not exist.*** Although OOR's website includes informing students of the right to file a complaint of FERPA	UCSF may be subject to unnecessary federal audits and reputational damage.	The Chancellor's Office, working in collaboration with the Privacy Office, Office of the Registrar, and potentially Student Affairs, should establish a process for filing	The Executive Vice Chancellor and Provost's Office and OOR will inquire about other campuses policies and practices around FERPA violation grievance processes, discuss

No.	Observation	Risk/Effect	Recommendation	MCA
	violation with the Department of Education (DOE), it is leading practice for an initial attempt of internal resolution to support the student's grievance and accountability before filing to DOE. Additionally, it is not made clear where or how to submit a FERPA complaint. UC PACAOS -110 requires a procedure to resolve student grievances about FERPA. While there are policies related to correcting information contained in records or grievances related to academic dismissals and disability accommodations, no policies or procedures related to access or disclosure were able to be identified during the review.	Students may not have sufficient information to exercise their rights under FERPA.	complaints that includes the following information: the date the alleged improper disclosure occurred or the date the parent learned of the disclosure; the name of the school official who made the disclosure, if that is known; the third party to whom the education records were disclosed; and the specific nature of the information disclosed. OOR should consider revising student's rights language to encourage an internal resolution process with a link to the internal procedure, while making DOE contact available on their website.	with relevant parties at UCSF to define ownership of the process, and delegate authority for developing a policy and procedure for handling FERPA violation grievances. **Responsible Party:** Communication Coordinator and Asst VC-Student Info **Implementation Date:** June 30, 2017
4	***Record-keeping requirements are not consistently interpreted or applied.*** While UC PACAOS-130 does provide instructions for recording and maintaining information on disclosures of student records and consent provision, the policy has been interpreted differently by OOR and the Schools' personnel responsible for handling requests. These different interpretations have led to differing practices across the groups receiving requests for student records, and potential incomplete maintenance of student record disclosures.	UCSF may not be able to provide evidence of compliance with FERPA if needed.	AAS requested clarification from Student Services at UCOP, who is currently corresponding with UCOP Office of General Counsel to provide feedback. OOR and the Schools should continue to work with UCOP to ensure that policies are interpreted and implemented appropriately, specifically regarding redisclosure notification requirements and record-keeping for disclosures and consent.	OOR will discuss at the next council meeting with other UC OOR offices and report back on the practice for record-keeping of consent and/or disclosure forms, including records of retention timeframe for records of disclosure and records of consent. **Responsible Party:** Asst VC-Student Info **Implementation Date:** June 30, 2017

C. Opportunities for Improvements

No.	Observation	Risk/Effect	Recommendation
1	***A single central access point or repository does not exist for student record requests.*** Student record requests can come in multiple places via multiple methods. This process is not conducive to tracking for fulfillment of disclosure request or managing and monitoring requests, which are key components for oversight activities. Strengthening oversight activities helps ensure restricted information is protected from unauthorized access.	The lack of oversight on all or at least high-risk type of student record requests that comes through the office hinders effectiveness of managing compliance.	If feasible, in order to reduce manual errors and administrative burden, determine an automated central place for submitting and receiving student record requests that enables reporting on types of requests and how they were handled to demonstrate compliance with FERPA.
2	***Clarifying the use of MedSIS flags to distinguish between internal records and records that would be disclosed to students and enhancing governance over the types of documents uploaded would strengthen FERPA compliance.*** Upon a student's request to inspect their records, MedSIS has a functionality that allows the system to zip all files except those that are flagged as "Progress" or "Office Use Only". The Student Record Administrator (SRA) then provides this auto-zipped file to the student in a secure location. However, the MedSIS User's Guide does not define when these flags should be used and their implication relating to FERPA education records. While it states "Faculty and staff members may also keep *informal* records related to their functional role with a student," most records in MedSIS would not be categorically exempt from disclosure to students based on FERPA requirements. There are about 70 users with roles including Staff Read-Only, Staff, Mentor, Director and Data Manager with ability to upload documents into MedSIS, and it's not always clear what types of document have been uploaded and flagged "Progress" or "Office Use Only". 486 students have documents labeled "Progress" that contain sensitive	Without clear definitions of what information should be flagged, individual users may flag different types of documents depending on their understanding, leading to incorrect provision of information to students.	SOM should assess the types of documents that have been flagged as internal records to understand current practices and determine if these documents are education or non-educational records that are not subject to student review. SOM should update their MedSIS user guide to explain when to use Progress or Office Use Only and their implications on FERPA compliance. SOM may want a category that flags "FERPA non-education" records if an assessment concludes that there is a business need to keep all records in MedSIS including those that are non-education as defined by FERPA to distinguish between records flagged as "Office Use Only" that may still be subject to student inspection. While corrective action was not required, SOM is committed to improving their processes, and will do the following by August 31, 2017: SOM will review the types of documents that have been flagged as internal records to understand current practices and determine if these documents are education or non- educational

No.	Observation	Risk/Effect	Recommendation
	disciplinary records. Without an actual walkthrough assessing these documents, SOM cannot be certain that internal documents that do not meet the FERPA definition of "education records" would be excluded from viewing by the student or that all documents that do meet the FERPA definition of "education records" would be included for viewing by the student.		records that are not subject to student review. SOM will update their MedSIS user guide to explain when to use Progress or Office Use Only and their implications on FERPA compliance. SOM will review and document current policy and practice for handling grievance related documentation in MedSIS including what roles can views these files and number of users with these roles. SOM will work with OOR and UCSF General Counsel to review the current process.