STUDENT HEALTH SERVICES

CALIFORNIA STATE UNIVERSITY,
SACRAMENTO

Audit Report 13-62
February 26, 2014

Members, Committee on Audit

Lupe C. Garcia, Chair
Steven M. Glazer, Vice Chair
Adam Day  Rebecca D. Eisen
Hugo N. Morales

Staff

Vice Chancellor and Chief Audit Officer: Larry Mandel
Senior Director: Michelle Schlack
Audit Manager: Ann Hough
IT Audit Manager: Greg Dove
Senior Auditors: Gordon Eng and Kim Pham

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
## CONTENTS

Executive Summary ........................................................................................................................................... 1

Introduction .................................................................................................................................................... 3
  Background .............................................................................................................................................. 3
  Purpose ................................................................................................................................................. 5
  Scope and Methodology ......................................................................................................................... 7

### OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Program Administration .............................................................................................................................. 9
  Policies and Procedures .......................................................................................................................... 9
  Educational Programs ........................................................................................................................... 9

Athletics Medicine ..................................................................................................................................... 10
  Policies and Procedures .................................................................................................................... 10
  Scope of Services ............................................................................................................................... 11

Information and Data Security ................................................................................................................ 12
  Vulnerability Management .................................................................................................................. 12
  Data Center Access ............................................................................................................................. 13
  Disposition of Protected Data ........................................................................................................... 14
  Disaster Recovery Plan ....................................................................................................................... 15
  System Backup and Recovery Procedures ......................................................................................... 16
CONTENTS

APPENDICES

APPENDIX A: Personnel Contacted
APPENDIX B: Campus Response
APPENDIX C: Chancellor’s Acceptance

ABBREVIATIONS

CSU California State University
CSUS California State University, Sacramento
DRP Disaster Recovery Plan
EMR Electronic Medical Records
EO Executive Order
HIPAA Health Insurance Portability and Accountability Act
ICSUAM Integrated California State University Administrative Manual
ISO Information Security Officer
IT Information Technology
OGC Office of General Counsel
OAAS Office of Audit and Advisory Services
SHC Student Health Centers
SHCS Student Health and Counseling Services
SHS Student Health Services
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of Audit and Advisory Services (OAAS) during the last quarter of 2012, the Board of Trustees, at its January 2013 meeting, directed that Student Health Services (SHS) be reviewed. The OAAS last reviewed Student Health Centers in 2000.

We visited the California State University, Sacramento campus from September 23, 2013, through October 25, 2013, and audited the procedures in effect at that time.

In our opinion, except for the effect of the weaknesses described below, the fiscal, operational, and administrative controls for SHS as of October 25, 2013, taken as a whole, were sufficient to meet the objectives stated in the “Purpose” section of this report. Areas of concern include: program administration, athletics medicine, and information and data security.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

The following summary provides management with an overview of conditions requiring attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [ ] refer to page numbers in the report.

PROGRAM ADMINISTRATION [9]

The campus health services oversight policy was last updated in 2008, and it contained information that conflicted with current practices and policies. Also, the campus did not obtain California State University Office of General Counsel approval for a single pharmacy rotational internship with three outside universities that provided health services at the Student Health and Counseling Services (SHCS).

ATHLETICS MEDICINE [10]

Athletics medicine policies and procedures were missing required medication administration provisions. Also, the scope of services and physician privileging in the athletics medicine department needed improvement. Specifically, the scope of services policy did not accurately reflect the services provided by campus athletics physicians and was not reviewed regularly. Further, physicians in athletics medicine were not subject to formal privileging to define their individual scope of services on behalf of the campus.

INFORMATION AND DATA SECURITY [12]

The campus was not following guidance for scanning servers and repairing vulnerabilities. Also, the campus did not maintain evidence of periodic, documented reviews of data center access. In addition, the campus could not provide evidence that all sensitive information maintained on SHCS computers was properly deleted prior to the computers’ disposition or redeployment. Further, the SHCS information technology (IT) disaster recovery plan (DRP) did not include sufficient detail to ensure the timely
recovery of SHCS systems. The campus also did not maintain documentation of the periodic testing of
the IT DRP, including testing of system backup and recovery procedures for the SHCS and athletics
medicine systems.
INTRODUCTION

BACKGROUND

The Policy of the Board of Trustees on Student Health Services was initially adopted in 1977 as a comprehensive systemwide policy; since then, it has been periodically revised and updated to reflect the changing regulatory, financial, and student demographic environments. In 1993, a task force study recommended that system roles, responsibilities, and expectations be recorded in executive orders (EO) issued by the chancellor, and the policy has been communicated in that format since that time.

The most recent version, EO 943, Policy on University Health Services, dated April 28, 2005, outlines the health services the campuses may provide, including the conditions that must be met to justify adding additional services or funding sources. It also describes operational expectations for pharmacies, staffing, facility cleanliness and safety, medical records management, and accreditation. The EO focuses primarily on the scope and activities of the student health centers (SHC) but also includes sections that are applicable to other campus programs providing student health care, such as intercollegiate athletics, due to the SHC audits conducted in 2000.

The primary health entity on each California State University (CSU) campus, the SHC, is funded by two mandatory student fees, which are covered in EO 1054, California State University Fee Policy, dated January 14, 2011: a health services fee covering basic health services available to students, and a health facilities fee to support the health center facility. These fees can be changed only after a student referendum or a consultation that allows meaningful input and feedback from appropriate campus constituents.

Every three years, each campus SHC and its pharmacy are required to obtain accreditation from a nationally recognized, independent review agency such as the Accreditation Association for Ambulatory Health Care. Pharmacies are also subject to periodic inspections by the California State Board of Pharmacy.

At the chancellor’s office, the student academic support department in the Academic Affairs division is responsible for monitoring systemwide SHC activities and ensuring that campus SHCs comply with CSU management and regulatory policies. In addition, a systemwide student health services advisory committee composed of the director or a designee from each campus SHC meets at least twice per year to provide recommendations to the chancellor regarding revisions to applicable EOs. The committee also identifies and implements corrective measures for issues identified in the systemwide survey and accreditation report reviews.

A majority of CSU campuses have implemented systems and applications that facilitate a transition to electronic medical records (EMR), including some vendor applications designed specifically for university health services. Privacy concerns surrounding these emerging technologies have brought about new regulations, including the Health Insurance Portability and Accountability Act (HIPAA), which establishes national standards for electronic health care transactions, and the Technology for Economic and Clinical Health Act, a part of the American Recovery and Reinvestment Act of 2009 that addresses the privacy and security concerns associated with the electronic transmission of health information. Although this audit assesses the security of medical records, it does not address HIPAA in depth, as the Office of Audit and Advisory Services (OAAS) reviewed the topic in 2010.
In 2000, the OAAS conducted an audit of SHC at ten campuses and issued a systemwide report. The report noted issues related to centralized oversight of student health activities, revisions to existing policies to clarify reporting and administrative expectations, credentialing of clinical staff in both the SHCs and athletics, and policies regarding the storage and dispensing of over-the-counter and prescription pharmaceuticals outside of campus pharmacies and in the athletics department. Recommendations from this audit were incorporated into EO 814, *Policy on University Health Services*, which was replaced by EO 943.
PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to student health services (SHS) activities and to determine the adequacy of controls that ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the audit objective, specific goals included determining whether:

- Administration of SHS is well-defined and includes clear lines of organizational authority and responsibility and documented delegations of authority.
- Policies and procedures relating to SHS are current and comprehensive, and are effectively communicated to appropriate stakeholders.
- Management consistently monitors and assesses the risks associated with providing SHS.
- The SHC is appropriately accredited.
- SHC clinical staff and other employees providing patient care possess the necessary credentials and qualifications, and designations are maintained in favorable standing with appropriate licensing boards and medical associations.
- SHS are appropriately defined and approved and are consistently provided to all eligible students and personnel.
- Health education programs are appropriately developed and communicated.
- Athletics medicine activities are conducted in accordance with campus and CSU policies.
- Pharmacy operations in the SHC and other areas providing SHS have obtained the appropriate licenses.
- Pharmacy formularies are limited to medications that are necessary to provide quality health care and are representative of those medications most effective in terms of treatment.
- Pharmacy security is maintained in accordance with CSU policy and state regulations.
- Pharmacy inventories are properly reported, safeguarded, and accounted for, and prescription dispensing and destruction controls are in accordance with CSU policies and state regulations.
- Medical records, including electronic records, are properly maintained, safeguarded, and retained.
- The security of student health facilities is maintained in accordance with campus and CSU policy.
 Health services fees are approved, used for designated purposes, and properly accounted for in accordance with CSU policy and directives.

 Senior management demonstrates an awareness of security risks and monitors the computer environment to ensure the security of medical records systems.

 Methods used to enforce user authentication and appropriate access assignments for EMR systems are effective.

 Access to electronic medical records systems, programs, and data is appropriately restricted, and facilities are appropriately protected from fire and power outages.

 Medical records systems purchased from outside vendors are subject to CSU security provisions during procurement, and external access by vendors is controlled.

 Information technology assets supporting SHS are appropriately protected, and all assets are accounted for and have a nominated owner responsible for their protection.

 Senior management has a plan to recover all systems supporting the SHC following a major disaster.
SCOPE AND METHODOLOGY

The proposed scope of the audit as presented in Attachment A, Audit Agenda Item 2 of the January 22 and 23, 2013, meeting of the Committee on Audit stated that Student Health Services includes the provision of basic and augmented health services through campus student health facilities and pharmacy operations. Proposed audit scope would include, but was not limited to, a review of compliance with federal and state laws, Trustee policy, and chancellor’s office directives; establishment of a student health advisory committee; accreditation status; staffing, credentialing, and re-credentialing procedures; safety and sanitation procedures, including staff training; budgeting procedures; fee authorization, cash receipt and disbursement controls, and trust fund management; pharmacy operations, security, and inventory controls; and the integrity and security of medical records.

Our study and evaluation were conducted in accordance with the International Standards for the Professional Practice of Internal Auditing, issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that accounting and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor policies, letters, and directives. The audit focused on procedures in effect from July 1, 2011, through October 25, 2013.

We focused primarily upon the internal administrative, compliance, and operational controls over SHS activities. Specifically, we reviewed and tested:

- Campus administration of SHS, including clear reporting lines and defined responsibilities, risk assessment, and current policies and procedures.
- SHC accreditation status and management responsiveness to recommendations made by the accreditation team.
- Procedures to confirm credentials and qualifications of clinical staff and other employees providing patient care.
- The definition and provision of basic and augmented health services in the SHC, including approval and eligibility for services.
- Health education programs for the student population.
- Administration of athletics medicine, including proper designation of responsible parties and the establishment of policies and procedures.
- Licensing and permit requirements for pharmacy operations at the SHC and other areas on campus, including athletics.
- Pharmacy formulary, dispensing, inventory, and physical security practices.
- Medical records management, including practices to ensure security and confidentiality.
Matters to ensure the security of student health facilities.

The establishment of and subsequent changes to the mandatory health services fee, and methods to set and justify fees for augmented services.

Budgets and financial records, including revenue and expenditure transactions in health fee trust accounts.

Policies and procedures to ensure that information technology facilities, hardware, systems, and applications used for SHS are adequately secured, both physically and logically.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

PROGRAM ADMINISTRATION

POLICIES AND PROCEDURES

The campus health services oversight policy was last updated in 2008, and it contained information that conflicted with current practices and policies.

Executive Order (EO) 943, Policy on University Health Services, dated April 28, 2005, states that the president or a designee shall ensure appropriate oversight of all university health services. It further states that on an annual basis, the campus president or designees shall submit copies of the campus oversight policy established by the president for all university health services to the chancellor’s office.

The vice president of planning, enrollment management, and student affairs stated that she has been working with the campus health oversight committee to update the campus health oversight policy.

Inadequate updating of policies and procedures increases the risk of injury to students and exposes the university to potential litigation and regulatory sanctions.

Recommendation 1

We recommend that the campus update the campus health services oversight policy.

Campus Response

We concur. Working with the Campus Health Oversight Committee, we will update the campus health services oversight policy by August 26, 2014.

EDUCATIONAL PROGRAMS

The campus did not obtain California State University (CSU) Office of General Counsel (OGC) approval for a single pharmacy rotational internship with three outside universities that provided health services at the SHCS.

EO 943, Policy on University Health Services, dated April 28, 2005, states that participation in educational programs that involve the provision of healthcare requires the approval of the president or designee, a contract or memorandum of understanding that has been approved by the CSU OGC, and oversight by the student health center director or designee.

The SHCS executive director stated that it was not campus procedure to obtain CSU OGC approval for intern/educational programs.

Improper approval of educational programs at SHCS exposes the campus to risks related to proper care of students and exposes the university to potential litigation.
Recommendation 2

We recommend that the campus obtain CSU OGC approval for educational programs that provide health services at the SHCS.

Campus Response

We concur. We will revise our procedures to include obtaining the approval of campus CSU OGC for all current health center educational programs by June 26, 2014.

ATHLETICS MEDICINE

POLICIES AND PROCEDURES

Athletics medicine policies and procedures were missing required medication administration provisions.

Specifically, we found that the policies did not address requirements that:

- Individuals receiving medications be properly informed about what they are taking, who prescribed the medication, and how they should take it.
- All emergency and travel kits be routinely inspected for drug quality and security, and a written protocol be developed to ensure compliance with the mandate.

EO 943, Policy on University Health Services, dated April 28, 2005, states that when pharmaceuticals are maintained for dispensing by a single licensed health care provider, written policies and procedures must be developed for storage, security, labeling, outdates, and recordkeeping, among others. In addition, individuals receiving medications shall be properly informed about what they are taking, who prescribed the medication, and how they should take it, and all emergency and travel kits shall be routinely inspected for drug quality and security, and a written protocol shall be developed to ensure compliance with this mandate.

The associate athletics director stated that these particular requirements were overlooked when the policy was developed.

Incomplete athletics medicine policies increase the risk of injury to student athletes and expose the university to potential litigation and regulatory sanctions.

Recommendation 3

We recommend that the campus update athletics medicine policies and procedures to address requirements that:
a. Individuals receiving medications be properly informed about what they are taking, who
prescribed the medication, and how they should take it.

b. All emergency and travel kits be routinely inspected for drug quality and security, and a written
protocol be developed to ensure compliance with the mandate.

Campus Response
We concur. Athletics will update their medicine policies and procedures to address these
requirements by May 26, 2014.

SCOPE OF SERVICES
The scope of services and physician privileging in the athletics medicine department needed
improvement.

Specifically, we found that:

- The scope of services policy for each specialty listed medical procedures that were not and would
not be expected to be practiced in the context of the physicians’ duties on campus. For example,
the orthopedist scope of services listed knee and hip replacements, and the dentist/oral surgeon
scope of services listed cleft lip and palate surgery.

- The campus could not provide evidence that the scope of services was being reviewed biennially.

- Physicians in athletics medicine were not subject to formal privileging to define their individual
scope of services on behalf of the campus.

EO 943, Policy on University Health Services, dated April 28, 2005, states that the scope of services
for each health care provider in athletics shall be in written protocols that are established on each
campus, and that the protocols shall cover student assistants, student athletic trainers, and other health
care providers for intercollegiate athletics. It further states that the protocols shall be reviewed
biennially and also, that only those who are qualified to provide health care shall be allowed to do so,
and that the president or designee, in conjunction with campus human resources, is responsible for
credentialing and privileging providers of health care in the athletic department.

The associate athletics director stated that the scope of services was created in response to EO 943,
which came out in 2005, and that the documents were created to show all the services the campus
athletic physicians were able to perform in case an injury occurred while an athlete was practicing or
competing for the campus and needed this specialized care. She also stated that the campus was not
clear as to who should be responsible for the biennial review. Further, the associate athletics director
stated that because the physicians generally see the students off-campus in their private offices, the
privileging they held for those practices was assumed to be sufficient.
Lack of a precise and approved scope of services and privileging of physicians for athletics medicine exposes the campus to confusion about service levels provided to campus athletes and could result in further injury to student athletes.

**Recommendation 4**

We recommend that the campus:

a. Update the scope of services for each specialty to remove medical procedures that are not and would not be expected to be practiced in the context of the physicians’ duties on campus.

b. Document biennial reviews of the scope of services.

c. Subject physicians in athletics medicine to formal privileging to define their individual scope of services on behalf of the campus.

**Campus Response**

We concur. By August 1, 2014, we will update our scope of services for each specialty and document its first review. The reviews will be biennial going forward. We will then obtain formal privileging documents for our athletic medicine physicians that will establish medical privileges granted based on their training, experience, and demonstrated competence specific to their scope of service.

**INFORMATION AND DATA SECURITY**

**VULNERABILITY MANAGEMENT**

The campus was not following guidance for scanning servers and repairing vulnerabilities.

We noted that:

- The campus did not conduct documented periodic reviews of vulnerability scans of SHCS and athletics servers with protected data and did not report vulnerabilities to system owners.

- SHCS and athletics medicine did not have procedures to appropriately address vulnerabilities in a timely manner.

CSUS *Vulnerability Scanning Procedures and Guidelines* states that system administrators must perform, analyze, remediate, or document exceptions and report on all maintenance scans completed on their systems. System administrators or designated department scan analysts must review all vulnerability scans for a system within 24 hours of scanning and are responsible for remediating vulnerabilities identified during vulnerability scanning. System administrators must also report their evaluation and remediation options to the system owner or designee upon completion of evaluation.
Integrated California State University Administrative Manual (ICSUAM) §8045.500, *Information Technology Security*, dated April 19, 2010, states that at a minimum, server administrators are required to scan regularly, remediate, and report unremediated vulnerabilities on critical systems or systems that store protected information within a prescribed time frame.

The information security officer (ISO) stated that the current processes and tools used to maintain SHCS and athletics medicine servers did not include reviewing vulnerability scanning results and addressing critical vulnerabilities.

Inadequate review of periodic vulnerability assessments may lead to compromise in network resources and loss of protected confidential information.

**Recommendation 5**

We recommend that the campus:

a. Conduct documented periodic reviews of vulnerability scans of SHCS and athletics medicine servers with protected data and report vulnerabilities to system owners.

b. Develop and implement procedures to appropriately address vulnerabilities in a timely manner.

**Campus Response**

We concur.

a. The campus’ information security office already conducts periodic campus-wide vulnerability reviews of campus servers with protected data. SHCS and athletics medicine will notify the ISO of the presence and location of all level one data on their systems. The ISO will ensure that servers that house SHCS and athletics data are included in future quarterly vulnerability scans. The ISO will provide vulnerability reports on the SHCS and athletics medicine servers with protected data to system owners after each campus-wide quarterly scan. The campus will complete all actions by May 26, 2014.

b. The system administrators of SHCS and athletics medicine will adopt and comply with existing campus-wide information security policies and procedures (i.e. Supplemental Information Security Policy 8045) and work with the campus information security office to both address any reported vulnerabilities in a timely manner and report completion of risk mitigation to the ISO. The campus will complete all actions by May 26, 2014.

**DATA CENTER ACCESS**

The campus did not maintain evidence of periodic, documented reviews of data center access.

ICSUAM §8080, *Physical Security*, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where information assets containing protected data are
stored. Campuses must protect these limited-access areas from unauthorized physical access while ensuring that authorized users have appropriate access. Campus information assets which access protected data that are located in public and non-public access areas must be physically secured to prevent theft, tampering, or damage. The level of protection provided must be commensurate with that of identifiable risks. Campuses must review and document physical access rights to campus limited-access areas annually.

The ISO stated that procedures to review data center access on an annual basis were in place; however, they did not include documentation of the process.

Lack of documentation for reviews of data center access increases the risk that a review will not be performed and that unauthorized personnel will have access to information assets.

**Recommendation 6**

We recommend that the campus maintain evidence of periodic, documented reviews of data center access.

**Campus Response**

In October 2013, the campus conducted and documented an annual review of the campus’ data center access. Previous audits and reviews, on at least an annual basis, have documented that the campus has met and exceeded the data access standards required. Additionally, the campus has contracted with a professional security firm to recommend and implement further best practices for data center security. The campus will provide documentation regarding both past and planned data center access reviews by May 1, 2014.

**DISPOSITION OF PROTECTED DATA**

The campus could not provide evidence that all sensitive information maintained on SHCS computers was properly deleted prior to the computers’ disposition or redeployment.

CSUS *Disposal of Protected Data Process*, dated August 15, 2010, states that local information technology staff members are responsible for logging the decommissioning and repurposing of all computers and devices in their area of responsibility.

ICSUAM §8065, *Information Asset Management*, dated April 19, 2010, states that campuses must maintain an inventory of information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. These assets must be categorized and protected throughout their entire life cycle, from origination to destruction.

The SHCS executive director stated that SHCS wiped all hard drives before they were transferred to property management; however, documentation of this process was not part of SHCS procedures. Additionally, she stated that the campus asset disposal and transfer form, which SHCS used to document asset transfers and disposals, did not include a section to document that the asset had been appropriately wiped.
Inadequate control over equipment assets, especially those containing protected data, increases the risk of loss, inappropriate use of state resources, and campus exposure to information security breaches.

**Recommendation 7**

We recommend that the campus maintain evidence that all sensitive information maintained on SHCS computers has been properly deleted prior to the computers’ disposition or redeployment.

**Campus Response**

We concur. Per the campus *Disposal of Protected Data Process*, SHCS will log the disposal of all sensitive data before decommissioning and repurposing of all computers and devices in their area by April 26, 2014.

**DISASTER RECOVERY PLAN**

The SHCS information technology (IT) disaster recovery plan (DRP) did not include sufficient detail to ensure the timely recovery of SHCS systems.

We found that:

- The IT DRP did not address emergency notification and escalation procedures for SHCS, nor did it include sufficient detail about recovery procedures for critical systems.

- The campus had not completed a business impact assessment for SHCS to determine the level of dependence on IT services and to ensure the timely recovery of critical systems.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, provides detailed guidance to campuses for creating, implementing, and maintaining a business continuity program that includes an IT DRP. It further states that goals, which must be met by such a program, include, but are not limited to, the listing, prioritizing, and establishing of recovery time objectives for essential functions, systems, and applications through business impact analysis and risk assessments. Campuses must keep all business continuity-related plans current, must test all plans for viability, and must reference all materials necessary to recover from a disaster.

ICSUAM §8085, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states that an information security program needs to support the maintenance and potential restoration of operations through and after both minor and catastrophic disruptions. Campuses must ensure that their information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users. Each campus must maintain an ongoing program that ensures the continuity of essential functions and operations following a catastrophic event. The campus program must be in compliance with the CSU Business Continuity Program.

The SHCS executive director stated that SHCS had a business continuity plan in place, but it needed additional refinement to address some of the concerns listed.
The absence of a comprehensive IT DRP increases the risk that business and data processing operations may not be restored within management expectations in the event of an emergency or disaster, which could result in financial and non-financial losses.

**Recommendation 8**

We recommend that the campus:

a. Revise the IT DRP to address emergency notification and escalation procedures for SHCS, and to include sufficient detail about recovery procedures for critical systems.

b. Complete a business impact assessment for SHCS to determine the level of dependence on IT services and to ensure the timely recovery of critical systems.

**Campus Response**

We concur. By August 1, 2014, SHCS will complete a business impact assessment to determine the level of dependence on IT services to ensure the timely recovery of any identified critical systems by adding to their existing business continuity plan. The existing approved IT DRP does not currently identify SHCS as a critical system. If SHCS’s business impact assessment recommends inclusion as a critical system, the campus will consider revising the IT DRP. Additionally, the current campus DRP procedures ensure timely recovery of non-critical systems.

**SYSTEM BACKUP AND RECOVERY PROCEDURES**

The campus did not maintain documentation of the periodic testing of the IT DRP, including testing of system backup and recovery procedures for the SHCS and athletics medicine systems.

ICSUAM §8085, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states that an information security program needs to support the maintenance and potential restoration of operations through and after both minor and catastrophic disruptions. Campuses must ensure that their information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users. Each campus must maintain an ongoing program that ensures the continuity of essential functions and operations following a catastrophic event. The campus program must be in compliance with the CSU Business Continuity Program.

The senior director of operations and system services stated that parts of the IT DRP, such as system backup and recovery procedures, were tested on a monthly basis; however, documentation of this testing was not part of procedures.

Lack of documentation addressing the periodic testing of the IT DRP, including system backup and recovery procedures, increases the risk that system backups will not be operable, which can result in a failure to recover systems in the event of a disaster.
Recommendation 9

We recommend that the campus maintain documentation of the periodic testing of the IT DRP, including testing of system backup and recovery procedures for the SHCS and athletics medicine systems.

Campus Response

We concur. The campus conducts annual tests of select critical aspects of its campus-wide IT DRP. The campus will provide documentation of the latest annual test by May 1, 2014. The system administrators of SHCS and athletics medicine will schedule with campus IT the periodic testing of SHCS and athletics medicine backup and recovery systems and maintain documentation by May 26, 2014.
# APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexander Gonzalez</td>
<td>President</td>
</tr>
<tr>
<td>Robin Carter</td>
<td>Associate Dean, College of Health and Human Services</td>
</tr>
<tr>
<td>Kendal Chaney-Buttleman</td>
<td>University Controller</td>
</tr>
<tr>
<td>Gina Curry</td>
<td>Director, Student Financial Services Center</td>
</tr>
<tr>
<td>Janet Dumonchelle</td>
<td>Pharmacist-in-Charge, Student Health and Counseling Services (SHCS)</td>
</tr>
<tr>
<td>Joseph Gengler</td>
<td>Information Technology Services Manager</td>
</tr>
<tr>
<td>Yavette Hayward</td>
<td>Senior Management Auditor</td>
</tr>
<tr>
<td>Justine Heartt</td>
<td>Associate Vice President for Financial Services</td>
</tr>
<tr>
<td>Emilene Holliday</td>
<td>Business Office Administrator, SHCS</td>
</tr>
<tr>
<td>Lisa Johnson</td>
<td>Associate Director, Clinical Operations</td>
</tr>
<tr>
<td>Ted Koubiar</td>
<td>Senior Director, Operations and System Services</td>
</tr>
<tr>
<td>Katherine Ledesma</td>
<td>Assistant to the Executive Director, SHCS</td>
</tr>
<tr>
<td>Ming-Tung (Mike) Lee</td>
<td>Vice President for Administration and Business Affairs/Chief Financial Officer</td>
</tr>
<tr>
<td>Lisa Johnson</td>
<td>Associate Director, Clinical Operations</td>
</tr>
<tr>
<td>Lois Mattice</td>
<td>Associate Athletics Director</td>
</tr>
<tr>
<td>Kaye Milburn</td>
<td>Director, Auditing Services</td>
</tr>
<tr>
<td>Darlene Spencer</td>
<td>Accreditation Coordinator and Credentialing</td>
</tr>
<tr>
<td>Joy Stewart-James</td>
<td>Executive Director, SHCS</td>
</tr>
<tr>
<td>Donald To</td>
<td>Information Technology Consultant, SHCS</td>
</tr>
<tr>
<td>Lori Varlotta</td>
<td>Vice President of Planning, Enrollment Management, and Student Affairs</td>
</tr>
<tr>
<td>Jeff Williams</td>
<td>Information Security Officer</td>
</tr>
</tbody>
</table>
March 28, 2014

Larry Mandel
Vice Chancellor and Chief Audit Officer
The California State University
401 Golden Shore
Long Beach, CA 90802-4210

SUBJECT: Campus Response to Audit Recommendations of Student Health Services, #13-62

Dear Larry:

Please find enclosed California State University, Sacramento’s response to the recommendations of the audit. The campus is committed to addressing and resolving the issues identified in the audit report.

If you have any questions or require additional information, please contact Kaye Milburn, Director of Auditing Services, at (916) 278-7439.

Sincerely,

Ming-Tung “Mike” Lee, Ph.D.
Vice President and Chief Financial Officer

MTL: sf

Enclosure

cc: Alexander Gonzalez, President
    Lori Varlotta, Vice President, Planning, Enrollment Management and Student Affairs
    Larry Gilbert, Vice President and Chief Information Officer
    Joy Stewart-James, Executive Director, Student Health and Counseling Services
    Jeff Williams, Information Security Officer and Senior Director, Customer Support
    Kaye Milburn, Director, Auditing Services
STUDENT HEALTH SERVICES
CALIFORNIA STATE UNIVERSITY,
SACRAMENTO
Audit Report 13-62

PROGRAM ADMINISTRATION

POLICIES AND PROCEDURES

Recommendation 1

We recommend that the campus update the campus health services oversight policy.

Campus Response

We concur. Working with the Campus Health Oversight Committee, we will update the campus health services oversight policy by August 26, 2014.

EDUCATIONAL PROGRAMS

Recommendation 2

We recommend that the campus obtain CSU OGC approval for educational programs that provide health services at the SHCS.

Campus Response

We concur. We will revise our procedures to include obtaining the approval of campus CSU OGC for all current health center educational programs by June 26, 2014.

ATHLETICS MEDICINE

POLICIES AND PROCEDURES

Recommendation 3

We recommend that the campus update athletics medicine policies and procedures to address requirements that:

a. Individuals receiving medications be properly informed about what they are taking, who prescribed the medication, and how they should take it.

b. All emergency and travel kits be routinely inspected for drug quality and security, and a written protocol be developed to ensure compliance with the mandate.
Campus Response

We concur. Athletics will update their medicine policies and procedures to address these requirements by May 26, 2014.

SCOPE OF SERVICES

Recommendation 4

We recommend that the campus:

a. Update the scope of services for each specialty to remove medical procedures that are not and would not be expected to be practiced in the context of the physicians' duties on campus.

b. Document biennial reviews of the scope of services.

c. Subject physicians in athletics medicine to formal privileging to define their individual scope of services on behalf of the campus.

Campus Response

We concur. By August 1, 2014, we will update our scope of services for each specialty and document its first review. The reviews will be biennial going forward. We will then obtain formal privileging documents for our athletic medicine physicians that will establish medical privileges granted based on their training, experience, and demonstrated competence specific to their scope of service.

INFORMATION AND DATA SECURITY

VULNERABILITY MANAGEMENT

Recommendation 5

We recommend that the campus:

a. Conduct documented periodic reviews of vulnerability scans of SHCS and athletics medicine servers with protected data and report vulnerabilities to system owners.

b. Develop and implement procedures to appropriately address vulnerabilities in a timely manner.

Campus Response

We concur.

a. Sacramento State's information security office already conducts periodic campus-wide vulnerability reviews of campus servers with protected data. SHCS and athletics medicine will notify the ISO of the presence and location of all level one data on their systems. The ISO will ensure that servers that house SHCS and athletics data are included in future quarterly vulnerability scans. The ISO will provide vulnerability reports on the SHCS and athletics...
medicine servers with protected data to system owners after each campus-wide quarterly scan. The campus will complete all actions by May 26, 2014.

b. The system administrators of SHCS and athletics medicine will adopt and comply with existing campus-wide information security policies and procedures (i.e. Supplemental Information Security Policy 8045) and work with the campus information security office to both address any reported vulnerabilities in a timely manner and report completion of risk mitigation to the ISO.

DATA CENTER ACCESS

Recommendation 6

We recommend that the campus maintain evidence of periodic, documented reviews of data center access.

Campus Response

In October 2013, the campus conducted and documented an annual review of Sacramento State’s data center access. Previous audits and reviews, on at least an annual basis, have documented that the campus has met and exceeded the data access standards required. Additionally, the campus has contracted with a professional security firm to recommend and implement further best practices for data center security. The campus will provide documentation regarding both past and planned data center access reviews by May 1, 2014.

DISPOSITION OF PROTECTED DATA

Recommendation 7

We recommend that the campus maintain evidence that all sensitive information maintained on SHCS computers has been properly deleted prior to the computers’ disposition or redeployment.

Campus Response

We concur. Per the campus Disposal of Protected Data Process, SHCS will log the disposal of all sensitive data before decommissioning and repurposing of all computers and devices in their area by April 26, 2014.

DISASTER RECOVERY PLAN

Recommendation 8

We recommend that the campus:

a. Revise the IT DRP to address emergency notification and escalation procedures for SHCS, and to include sufficient detail about recovery procedures for critical systems.

b. Complete a business impact assessment for SHCS to determine the level of dependence on IT services and to ensure the timely recovery of critical systems.
Campus Response

We concur. By August 1, 2014, SHCS will complete a business impact assessment to determine the level of dependence on IT services to ensure the timely recovery of any identified critical systems by adding to their existing business continuity plan. The existing approved IT DRP does not currently identify SHCS as a critical system. If SHCS's business impact assessment recommends inclusion as a critical system, the campus will consider revising the IT DRP. Additionally, the current campus DRP procedures ensure timely recovery of non-critical systems.

SYSTEM BACKUP AND RECOVERY PROCEDURES

Recommendation 9

We recommend that the campus maintain documentation of the periodic testing of the IT DRP, including testing over system backup and recovery procedures for the SHCS and athletics medicine systems.

Campus Response

We concur. Sacramento State conducts annual tests of select critical aspects of its campus-wide IT DRP. The campus will provide documentation of the latest annual test by May 1, 2014. The system administrators of SHCS and athletics medicine will schedule with campus IT the periodic testing of SHCS and athletics medicine backup and recovery systems and maintain documentation by May 26, 2014.
April 21, 2014

MEMORANDUM

TO: Mr. Larry Mandel  
Vice Chancellor and Chief Audit Officer

FROM: Timothy P. White  
Chancellor

SUBJECT: Draft Final Report 13-62 on Student Health Services, California State University, Sacramento

In response to your memorandum of April 21, 2014, I accept the response as submitted with the draft final report on Student Health Services, California State University, Sacramento.

TPW/amd