CONTENTS

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

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

OBSERVATIONS, RECOMMENDATIONS,
AND CAMPUS RESPONSES

Program Administration ................................................................................................................... 9
  Governance ................................................................................................................................. 9
  Accreditation ............................................................................................................................. 10
  Credentialing ............................................................................................................................ 11
  Prescription Pad Controls .......................................................................................................... 12

Athletics Medicine .......................................................................................................................... 13
  Governance ............................................................................................................................... 13
  Scope of Services Protocol ......................................................................................................... 15
  Pharmacy Policies ...................................................................................................................... 15

Pharmacy .......................................................................................................................................... 17

Information and Data Security ....................................................................................................... 17
  Information Security Awareness Training ............................................................................... 17
  Network Segmentation .............................................................................................................. 18
  Encryption ................................................................................................................................. 19
  Vulnerability Management ........................................................................................................ 20
  System Access Controls ............................................................................................................ 21
  Disaster Recovery Plan ............................................................................................................... 22
## APPENDICES

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

## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO</td>
<td>Chancellor’s Office</td>
</tr>
<tr>
<td>CSU</td>
<td>California State University</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>EMR</td>
<td>Electronic Medical Records</td>
</tr>
<tr>
<td>EO</td>
<td>Executive Order</td>
</tr>
<tr>
<td>ICSUAM</td>
<td>Integrated California State University Administrative Manual</td>
</tr>
<tr>
<td>IS</td>
<td>Information Security</td>
</tr>
<tr>
<td>ISO</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>OAAS</td>
<td>Office of Audit and Advisory Services</td>
</tr>
<tr>
<td>SA</td>
<td>Student Affairs</td>
</tr>
<tr>
<td>SAM</td>
<td>State Audit Manual</td>
</tr>
<tr>
<td>SDSM</td>
<td>San Diego Sports Medicine and Family Health Center</td>
</tr>
<tr>
<td>SDSU</td>
<td>San Diego State University</td>
</tr>
<tr>
<td>SHC</td>
<td>Student Health Center</td>
</tr>
<tr>
<td>SHS</td>
<td>Student Health Services</td>
</tr>
</tbody>
</table>
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 San Diego State University 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, athletic medicine, pharmacy, 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]

Governance of student health services required improvement. For example, responsibility for university health services provided in some areas was not adequately documented, and the campus health services oversight policy was not submitted to the chancellor’s office (CO) on an annual basis. In addition, the San Diego State University (SDSU) student health services (SHS) accreditation process needed improvement. Specifically, the re-accreditation process was incomplete, and the campus could not provide evidence that the 2010 accreditation report had been forwarded to the campus president or designee and the CO. Further, administration of medical staff credentials required improvement. For example, the SHS credentialing policy was outdated and did not reflect current credentialing review practices, the SHS did not maintain a credentialing file on the director of athletic medicine, and credentialing files for SHS staff were not always current. Also, prescription pad security needed improvement. Specifically, blank prescription pads were stored in a locked cabinet within the pharmacy, but the key was stored in an open space behind the counter, and the campus did not perform periodic inventories of the prescription pad stock or reconciliations of the pads to the physician sign-out logbook.

ATHLETICS MEDICINE [13]

The relationship between SHS and the athletics was not adequately defined. We found that there was no current documentation defining the relationship between SHS and athletics medicine, including the roles, responsibilities, reporting structure, athletics medicine director’s accountability to the SHS medical director, and funding arrangements. Also, the scope of services protocol for athletic medicine was not
being reviewed biennially. In addition, athletics pharmacy policies were not up to date, and did not include formal inventory procedures, a written protocol that describes the removal and disposal of medications, or a policy for inspecting travel kits.

PHARMACY [17]

The campus policy for pharmaceutical requests did not address the requirement that formulary content be reviewed at least annually or name the person who would perform the review, and it had not been finalized.

INFORMATION AND DATA SECURITY [17]

SHS did not train all employees with access to protected data in information security awareness. Also, the campus did not place SHS servers containing protected information on a separate network segment from user computers. Additionally, the campus did not encrypt sensitive data maintained in the electronic medical records and dental systems. Further, the campus did not perform periodic vulnerability scans of SHS servers connected to the campus network. In addition, administration of privileged and user access to systems containing protected data needed improvement. For example, the campus did not maintain a complete inventory of user accounts with privileged access; periodic, documented management reviews of privileged and user accounts within all systems containing protected data were not performed, and access to protected information in the electronic medical records and dental systems was not restricted to individuals on a need-to-know basis. Also, the campus did not have a written information technology disaster recovery plan (DRP) for SHS computer 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.
Measures 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

GOVERNANCE

Governance of student health services required improvement.

We found that:

› Responsibility for university health services provided in areas such as student affairs, academic affairs, athletics, and the Imperial Valley campus was not documented with a written designation or delegation of authority from the president.

› The campus health services oversight policy was not submitted to the chancellor’s office (CO) on an annual basis.

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 CO.

The associate vice president for student affairs stated that a formal delegation had not been established and the policy had not been submitted to the CO due to oversight.

A lack of clear accountability increases the risk that campus oversight will not include the entire range of university health services available on the campus.

Recommendation 1

We recommend that the campus:

a. Document responsibility for university health services provided in areas such as student affairs, academic affairs, athletics, and the Imperial Valley campus with a written designation or delegation of authority from the president.

b. Submit the campus health services oversight policy to the CO on an annual basis.

Campus Response

We concur.

a. The campus will document responsibility for university health services with a written delegation of authority from the president. This will be completed by April 30, 2014.
b. The campus health services oversight policy will be submitted to the CO by April 30, 2014, and then annually as required.

ACCREDITATION

The San Diego State University (SDSU) student health services (SHS) accreditation process needed improvement.

We found that:

- The re-accreditation process was incomplete. Accreditation for the SDSU SHS expired in June 2013, and although SHS management requested and received an extension on the re-accreditation deadline, that deadline was not met.

- The campus could not provide evidence that the 2010 accreditation report had been forwarded to the campus president or designee and the CO.

EO 943, Policy on University Health Services, dated April 28, 2005, states that each SHC shall be evaluated and accredited by an appropriate, nationally recognized, independent review agency and that re-accreditation evaluations shall be conducted at three-year intervals. It further states that the accrediting agency’s report shall be sent to the campus president or designee and to the CO.

The SHS director stated that the department requested the delay in the accreditation review because additional preparation time was needed due to turnover in management and key staff. He further stated that due to the turnover, the staff has not been able to provide evidence showing that the 2010 accreditation report was forwarded to the campus president and CO.

Lapse of accreditation and lack of evidence showing that the required accreditation report was forwarded to the campus president and CO undermines management’s ability to monitor the quality of health services provided at the SHS.

Recommendation 2

We recommend that the campus:

a. Complete the re-accreditation process.

b. Maintain evidence showing that accreditation reports have been forwarded to the campus president or designee and the CO.

Campus Response

We concur. The re-accreditation process has been completed and the reports have been sent to the president and the CO.
CREDENTIALING

Administration of medical staff credentials required improvement.

We found that:

- The SHS credentialing policy was outdated and did not reflect current credentialing review practices.
- The SHS did not maintain a credentialing file on the director of athletic medicine, who was under the direct supervision of the SHS medical director.
- Credentialing files for SHS staff were not always current. We reviewed ten SHS employee credentialing files and found that:
  - None of the files contained appointment or reappointment letters.
  - None of the files contained the peer review subcommittee summary of findings for each appointee at the time of reappointment.
  - Peer review results were not signed or dated in any of the files.
  - The checklist used to document the verification of file requirements, such as current license and board certification, was not completed for any of the files.

EO 943, Policy on University Health Services, dated April 28, 2005, states that the student health center director or designee, in conjunction with campus human resources, is responsible for the credentialing and privileging of providers of health care in the student health center.

SHS Policy AD/VII/2, Credentialing, Clinical Appointments and Clinical Privileges Policies and Procedures, dated July 9, 2006, states credential files maintained for each healthcare professional should include the initial application, reapplication, verifications, privileges granted, and other pertinent information as required by SHS.

State Administrative Manual (SAM) §20050 states that systems of internal control deficiencies include policy and procedural or operational manuals that are not currently maintained.

The SHS director of clinical services stated that the policy and credentialing files were not regularly reviewed due to extended management turnover. He further stated that a staff member had already been assigned the review of files, but had not been able to complete the duty prior to the start of the audit.

Outdated policies and procedures may result in confusion about expected requirements, and inadequate monitoring of credentials exposes the campus to risks related to proper care of students and exposes the university to potential litigation.
**Recommendation 3**

We recommend that the campus:

a. Update the SHS credentialing policy to reflect current credentialing review practices.
b. Create and maintain a credentialing file for the director of athletic medicine.
c. Maintain current credentialing files for all SHS staff, with the required documentation.

**Campus Response**

We concur.

a. The campus will update the SHS credentialing policy by July 1, 2014.
b. The campus will create and maintain a credentialing file for the director of athletic medicine by July 1, 2014.
c. The campus will maintain current credentialing files for all SHS staff, with the required documentation, by July 1, 2014.

**PRESCRIPTION PAD CONTROLS**

Prescription pad security needed improvement.

Specifically, we found that:

- Blank prescription pads were stored in a locked cabinet within the pharmacy, but the key was stored in an open space behind the counter.
- The campus did not perform periodic inventories of the prescription pad stock or reconciliations of the pads to the physician sign-out logbook.

SAM §20050 states that the elements of a satisfactory system of internal control and administrative controls shall include an established system of practices to be followed in performance of duties and a system of authorization and recordkeeping procedures adequate to provide effective accounting control.

Government Codes §13402 and 13403 state that management is responsible for establishing and maintaining a system of internal controls, which includes documenting the system, communicating system requirements to employees, and assuring that the system is functioning as prescribed.

The SHS medical director stated his belief that pharmacy access security measures appeared sufficient to safeguard the stock of prescription pads within the pharmacy. He also stated that the sign-out log process made it readily apparent which pre-numbered prescription pads were in stock. He further stated that although sign outs were occasionally not in numerical order, there was sufficient accountability for inventory purposes.
Lack of adequate security, inventories, and reconciliations of prescription pads increases the risk of theft and unauthorized usage.

**Recommendation 4**

We recommend that the campus:

a. Store the key to the prescription pad cabinet in a secure location.

b. Perform periodic inventories of the prescription pad stock and reconciliations of the pads to the physician sign-out logbook.

**Campus Response**

We concur.

a. The key to the prescription pad cabinet is now in a secured location.

b. An inventory of the prescription pad stock and reconciliation of the pads have been conducted and will continue to be performed periodically.

**ATHLETICS MEDICINE**

**GOVERNANCE**

The relationship between SHS and athletics medicine was not adequately defined.

We found that:

- There was no current documentation defining the relationship between SHS and athletics medicine, including the roles, responsibilities, reporting structure, athletics medicine director’s accountability to the SHS medical director, and funding arrangements. A memorandum of understanding that outlined the roles and responsibilities of each party expired in 2007.

- The campus could not provide evidence that the president or designee had designated a physician responsible for medical oversight of the athletics medicine program. The contract with San Diego Sports Medicine and Family Health Center (SDSM), which assigned medical oversight to the athletics medical director, was signed by the former associate vice president of financial operations.

- There was no documentation outlining who was responsible for the direct supervision of consulting physicians who were working for athletics medicine but were not part of the SDSM arrangement.
The scope of services policy was unclear regarding the role of the SHS medical director in athletics medicine.

EO 943, *Policy on University Health Services*, dated April 28, 2005, states that the president or designee is responsible for ensuring appropriate oversight of all medical services provided to students participating in intercollegiate athletics on each campus. It further states that the scope of service for each healthcare provider shall be in written protocols that are established on each campus.

The SHS director stated that the lack of written designation from the university president was due to oversight. The SHS director of clinical services stated that recent changes to the business model addressing the retention of team physicians resulted in a delay in updating policies, procedures, and organizational charts to reflect the current practice.

A lack of clear accountability increases the risk of inadequate health administration and patient care.

**Recommendation 5**

We recommend that the campus:

a. Document the relationship between SHS and athletics, including the roles, responsibilities, reporting structure, athletics medicine director’s accountability to the medical director at SHS, and funding arrangements.

b. Obtain written designation from the president or designee of the physician responsible for medical oversight of the athletics medicine program.

c. Document who is responsible for the direct supervision of the consulting physicians who are working for athletics medicine but are not part of the SDSM arrangement.

d. Update the scope of services policy to clarify the role of the SHS medical director in athletics medicine.

**Campus Response**

We concur.

a. The campus will document the relationship between SHS and athletics as outlined by July 1, 2014.

b. The campus will obtain written designation from the president or designee of the physician responsible for medical oversight of the athletics medicine program by July 1, 2014.

c. The campus will document who is responsible for the direct supervision of the consulting physicians who are working for athletics medicine but are not part of the SDSM arrangement by July 1, 2014.
d. The campus will update the scope of services policy to clarify the role of the SHS medical
director in athletics medicine by July 1, 2014.

SCOPE OF SERVICES PROTOCOL

The scope of services protocol for athletics medicine was not being reviewed biennially.

We found that there was a gap of several years between the last two documented reviews.

EO 943, *Policy on University Health Services*, dated April 28, 2005, states that athletics medicine
shall have a scope of service in a written protocol that covers all parties involved in athlete care, and
that these protocols shall be reviewed biennially.

The SHS medical director stated that the failure to document policy reviews was due to oversight
during a time when the director of athletics medicine was repeatedly absent for long periods and
arrangements for redistribution of all his responsibilities had not yet been made.

Inadequate review of the scope of services protocol increases the risk that current practices will not be
properly reflected and exposes the campus to potential litigation.

Recommendation 6

We recommend that the campus review the scope of services protocol for athletics medicine biennially.

Campus Response

We concur. The campus will review the scope of services protocol for athletics medicine biennially.
The first review will be completed by July 1, 2014.

PHARMACY POLICIES

Athletics pharmacy policies were not up to date.

We found that policies did not include:

- Provisions for formal inventory procedures that compared expected stock to actual stock and
recorded and accounted for variances.

- A written protocol that described the removal and disposal of outdated, deteriorated, or recalled
medications.

- A policy describing the practice for inspecting travel kits and maintaining a log documenting such
inspections.
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 shall be developed for storage, security, labeling, outdates, recordkeeping, and other applicable California law. It further states that all drug stock shall be examined at regular intervals for removal of outdated, deteriorated, or recalled medications. Inventories shall be conducted at least annually in order to purge outdated, deteriorated, and recalled medications and to maintain formularies consistent with California State University (CSU) policy. A written protocol for reviewing all drug stock shall be established and available for review. All emergency and travel kits containing medications and over-the-counter drugs shall be routinely inspected for drug quality and security. A written protocol and log shall be maintained to ensure compliance with this mandate.

The SHS medical director stated that inventory policy update delays were due to discussions among the athletics medicine parties on how to best control pharmaceuticals within the area, and there was a delay in recording and disseminating the new control process. He further stated that although the policies were not in writing, the athletics training staff routinely conducted inventories.

A lack of written athletics medicine policies increases the risk that current practices will be misunderstood and exposes the campus to potential litigation.

**Recommendation 7**

We recommend the campus update athletics pharmacy policies to include:

a. Provisions for formal inventory procedures that compare expected stock to actual stock and record and account for variances.

b. A written protocol that describes the removal and disposal of outdated, deteriorated, or recalled medications.

c. A policy describing the practice for inspecting travel kits and maintaining a log documenting such inspections.

**Campus Response**

We concur.

a. The campus will establish formal inventory procedures that compare expected stock to actual stock and record and account for variances. This will be completed by April 30, 2014.

b. The campus will establish a written protocol that describes the removal and disposal of outdated, deteriorated, or recalled medications. This will be completed by April 30, 2014.

c. The campus will establish a policy describing the practice for inspecting travel kits and maintaining a log documenting such inspections. This will be completed by April 30, 2014.
PHARMACY

The campus policy for pharmaceutical requests did not address the requirement that formulary content be reviewed at least annually or name the person who would perform the review, and it had not been finalized.

EO 943, Policy on University Health Services, dated April 28, 2005, states that student health centers have formularies that are limited to medication necessary to provide quality health care and are representative of those medications most effective in terms of treatment. It further states that consideration shall be given to cost and quality factors in determining which medications shall be included in the formulary, that the formulary content shall include prescription and non-prescription items, and that it shall be reviewed at least annually.

The SHS medical director stated that the delay in obtaining approval for the policy was due to turnover in management and key staff. He further stated that the omission of the annual review provision would likely have been caught during the review process.

Unclear policies increase the risk that current practices will be misunderstood and expose the campus to potential litigation.

Recommendation 8

We recommend the campus update its policy for pharmaceutical requests to address the requirement that formulary content be reviewed at least annually and name the person who will perform the review, and finalize the policy.

Campus Response

We concur. The campus will update its policy to include the requirement to review formulary content at least annually, to identify the person who will perform the review, and to finalize the policy. This will be completed by April 30, 2014.

INFORMATION AND DATA SECURITY

INFORMATION SECURITY AWARENESS TRAINING

The campus did not train all SHS employees with access to protected data in information security awareness.

Integrated California State University Administrative Manual (ICSUAM) §8035, Information Security Awareness and Training, dated April 19, 2010, states that all employees with access to protected data and information assets must participate in appropriate information security awareness training. When appropriate, information security training must be provided to individuals whose job functions require specialized skill or knowledge in information security.
The information security officer (ISO) stated that the university had been waiting for the new CSU information security training to be released. She further stated that in the meantime, the focus had been on providing industry-specific training, such as Health Insurance Portability and Accountability Act training, in order to mitigate key risks.

Inadequate administration of information security awareness training for employees with access to computer resources increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.

**Recommendation 9**

We recommend that the campus train all employees with access to protected data in information security awareness.

**Campus Response**

We concur. The campus will train all SHS employees with access to protected data in information security awareness by April 30, 2014.

**NETWORK SEGMENTATION**

The campus did not place SHS servers containing protected information on a separate network segment from user computers.

ICSUAM §8045.100, *Information Technology Security*, dated April 19, 2010, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

ICSUAM §8045.300, *Information Technology Security*, dated April 19, 2010, states that campuses must appropriately design their networks based on risk, data classification, and access in order to ensure the confidentiality, integrity and availability of their information assets. Each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

The director of technology services for student affairs (SA) stated that the campus recently reorganized the SA function, which oversees SHS. He further stated that as a result, SA was in the process of assessing the SHS information technology (IT) environment to ensure compliance with campuswide policies, including segmenting user computers from sensitive servers.

Placing servers with sensitive information on the same network as internal systems increases the risk of compromise and unauthorized access to protected data.
Recommendation 10

We recommend that the campus place SHS servers containing protected data on a separate network segment from user computers.

Campus Response

We concur. The campus is implementing a plan to separate the servers and user computers into separate network segments, and will accept the associated risks until implementation is completed.

ENCRIPTION

The campus did not encrypt sensitive data maintained in the electronic medical records and dental systems.

SDSU Information Security (IS) Plan 3.9.6, Use of Databases, dated February 2013, states that IT managers are responsible for ensuring that access to protected information in databases is approved according to required job duties. Access control should include a combination of file read/write privileges and access control lists on the database data objects. Databases should be configured to encrypt protected level 1 elements.

ICSUAM §8045, Information Technology Security, dated April 19, 2010, states that each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats. Additionally, each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

The director of technology services for SA stated that the campus recently reorganized the SA function, which oversees SHS. He further stated that as a result, SA was in the process of assessing the SHS IT environment to ensure compliance with campuswide policies, including database encryption.

Lack of encryption for protected data in storage increases the risk of loss or inappropriate use of such data and increases the risk of information security breaches, which could require the campus to notify all affected parties, adversely affecting the campus’ reputation.

Recommendation 11

We recommend that the campus encrypt sensitive data maintained in the electronic medical records and dental systems.
Campus Response

We concur. The campus is implementing a plan to work with vendors and upgrade the systems to encrypt sensitive medical and dental system records, and will accept the associated risks until implementation is completed.

VULNERABILITY MANAGEMENT

The campus did not perform periodic vulnerability scans of SHS servers connected to the campus network.

SDSU IS Plan 3.99, IT Security Office Assessments, dated February 2013, states that as part of its university responsibilities, the IT security office will conduct security assessments of departmental operations, which may include, but are not limited to, review of network security and information security. All vulnerabilities identified during the assessment will be documented by the IT security office for review with the applicable IT manager and IT support staff. IT managers will be responsible for remediating any critical vulnerabilities immediately; creating mitigation plans and estimated completion dates for all serious vulnerabilities within two weeks of the review meeting; indicating assumed risk for vulnerabilities that cannot be mitigated, but must remain in production; and notifying users when there is a security conflict with the system use.

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 director of technology services for SA stated that the campus recently reorganized the SA function, which oversees SHS. He further stated that as a result, SA was in the process of assessing the SHS IT environment to ensure compliance with campuswide policies, including performing and reviewing vulnerability assessments on a periodic basis.

Lack of periodic vulnerability assessments may lead to a compromise of network resources and loss of protected confidential information.

Recommendation 12

We recommend that the campus perform periodic vulnerability scans of SHS servers connected to the campus network.

Campus Response

We concur. The campus will perform, by July 1, 2014, periodic vulnerability scans of SHS servers connected to the campus network.
SYSTEM ACCESS CONTROLS

Administration of privileged and user access to systems containing protected data needed improvement.

We found that:

- The campus did not maintain a complete inventory of user accounts with privileged access.

- Periodic, documented management reviews of privileged and user accounts within all systems containing protected data were not performed.

- Access to protected information in the electronic medical records and dental systems was not restricted to individuals on a need-to-know basis.

SDSU IS Plan 3.6.1.1, *Creating and Assigning Accounts*, dated February 2013, states that privileged accounts must be reviewed and reapproved annually.

SDSU IS Plan 3.6.1.3, *Reviewing, Disabling, Reassigning, or Deleting Accounts*, dated February 2013, states that access-approving managers should be notified whenever an employee is terminated and should periodically review access to detect unauthorized access or user access that exceeds an employee’s current job responsibilities. Access to critical information assets or assets containing protected level 1 or 2 data must be reviewed annually, and the review must be documented.


ICSUAM §8060.400, *Access Control*, dated April 19, 2010, states that campuses must develop procedures to detect unauthorized access and privileges assigned to authorized users that exceed the required access rights needed to perform their job functions. Appropriate campus managers and data owners must review, at least annually, user access rights to information assets containing protected data. The results of the review must be documented.

ICSUAM §8060.200, *Access Control*, dated April 19, 2010, states that access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of need-to-know and least privilege.

The director of technology services for SA stated that the campus recently reorganized the SA function, which oversees SHS. He further stated that as a result, SA was in the process of assessing the SHS IT environment to ensure compliance with campuswide policies, including performing periodic reviews of user accounts and limiting access to protected data to individuals with a need to know.

Lack of periodic, documented reviews of privileged and user accounts and improper access to sensitive data increases the risk of inadequate segregation of duties and unauthorized or inappropriate
exposure to sensitive data, which can adversely affect campus compliance with existing regulations regarding protection of such data.

**Recommendation 13**

We recommend that the campus:

a. Maintain a complete inventory of user accounts with privileged access.

b. Perform periodic, documented management reviews of privileged and user accounts within all systems containing protected data.

c. Restrict access to protected information in the electronic medical records and dental systems to individuals on a need-to-know basis.

**Campus Response**

We concur.

a. The campus will maintain a complete inventory of user accounts with privileged access by April 30, 2014.

b. The campus will perform periodic, documented management reviews of privileged and user accounts within all systems containing protected data. This will be completed by April 30, 2014.

c. The campus will restrict access to protected information in the electronic medical records and dental systems to individuals on a need-to-know basis. This will be completed by April 30, 2014.

**DISASTER RECOVERY PLAN**

The campus did not have a written IT disaster recovery plan (DRP) for SHS computer 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. The campus 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 director of technology services for SA stated that the campus recently reorganized the SA function, which oversees SHS. He further stated that as a result, SA was in the process of assessing the SHS IT environment to ensure compliance with campuswide policies, including developing an IT DRP for SHS systems.

The absence of a written IT DRP increases the risk that business and data processing operations may not be restored within a reasonable time frame in the event of an emergency or disaster and can create recovery delays that result in unnecessary financial and non-financial losses.

**Recommendation 14**

We recommend that the campus develop a written IT DRP for SHS computer systems.

**Campus Response**

We concur. The campus will develop the IT DRP by July 1, 2014.
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elliot Hirshman</td>
<td>President</td>
</tr>
<tr>
<td>Juan Abenojar</td>
<td>Financial Analyst, Student Health Services (SHS)</td>
</tr>
<tr>
<td>Reginald Blaylock</td>
<td>Associate Vice President, Student Affairs</td>
</tr>
<tr>
<td>Jenny Bramer</td>
<td>Associate Athletic Director</td>
</tr>
<tr>
<td>Valerie Carter</td>
<td>Director, Audit and Tax</td>
</tr>
<tr>
<td>Tony Chung</td>
<td>Director, Technology Services, Student Affairs</td>
</tr>
<tr>
<td>Gene DeLuc</td>
<td>Technology Security Officer</td>
</tr>
<tr>
<td>Netta Glover</td>
<td>Administrative Coordinator, SHS</td>
</tr>
<tr>
<td>Susan Henry</td>
<td>Administrative Manager, SHS</td>
</tr>
<tr>
<td>Russell Klinkenberg</td>
<td>Director, SHS (At time of review)</td>
</tr>
<tr>
<td>Lorretta Leavitt</td>
<td>Associate Vice President, Financial Operations</td>
</tr>
<tr>
<td>Gregg Lichtenstein</td>
<td>Director, SHS</td>
</tr>
<tr>
<td>Irma Martinez</td>
<td>Imperial Valley Campus Director, Business and Financial Services</td>
</tr>
<tr>
<td>Tom McCarron</td>
<td>Vice President, Business and Financial Affairs</td>
</tr>
<tr>
<td>Dana McCoy</td>
<td>Manager, Accounting Services</td>
</tr>
<tr>
<td>Kim Reilly</td>
<td>Assistant Controller</td>
</tr>
<tr>
<td>Shelby Stanfill</td>
<td>Family Pact Coordinator</td>
</tr>
<tr>
<td>Felecia Vlahos</td>
<td>Information Security Officer</td>
</tr>
</tbody>
</table>
February 6, 2014

Mr. Larry Mandel
Vice Chancellor and Chief Audit Officer
Office of Audit and Advisory Services
The California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802

Dear Mr. Mandel:

Attached is San Diego State University’s response to Audit Report 13-60, Student Health Services. Documentation of policy and control changes will follow under separate cover.

Should you have any questions or require additional information, please contact Valerie Carter, Audit and Tax Director, at 619-594-5901.

Sincerely,

[Signature]

Tom McCarron
Vice President and CFO, Business and Financial Affairs

Attachment

c: Elliot Hirshman, President
   Eric Rivera, Vice President, Student Affairs
   Reginald Blaylock, Associate Vice President, Student Affairs
   Gregg Lichtenstein, Director, Student Health Services
   Tony Chung, Director, Technology Services, Student Affairs
   Valerie Carter, Director, Audit and Tax
PROGRAM ADMINISTRATION

GOVERNANCE

Recommendation 1

We recommend that the campus:

a. Document responsibility for university health services provided in areas such as student affairs, academic affairs, athletics, and the Imperial Valley campus with a written designation or delegation of authority from the president.

b. Submit the campus health services oversight policy to the CO on an annual basis.

Campus Response

We concur.

a. The campus will document responsibility for university health services with a written delegation of authority from the president. This will be completed by April 30, 2014.

b. The campus health services oversight policy will be submitted to the CO by April 30, 2014 and then annually as required.

ACCREDITATION

Recommendation 2

We recommend that the campus:

a. Complete the re-accreditation process.

b. Maintain evidence showing that accreditation reports have been forwarded to the campus president or designee and the CO.

Campus Response

We concur. The re-accreditation process has been completed and the reports have been sent to the president and the CO.
CREDENTIALING

Recommendation 3

We recommend that the campus:

a. Update the SHS credentialing policy to reflect current credentialing review practices.
b. Create and maintain a credentialing file for the director of athletic medicine.
c. Maintain current credentialing files for all SHS staff, with the required documentation.

Campus Response

We concur.

a. The campus will update the SHS credentialing policy by July 1, 2014.
b. The campus will create and maintain a credentialing file for the director of athletic medicine by July 1, 2014.
c. The campus will maintain current credentialing files for all SHS staff, with the required documentation, by July 1, 2014.

PRESCRIPTION PAD CONTROLS

Recommendation 4

We recommend that the campus:

a. Store the key to the prescription pad cabinet in a secure location.
b. Perform periodic inventories of the prescription pad stock and reconciliations of the pads to the physician sign-out logbook.

Campus Response

We concur.

a. The key to the prescription pad cabinet is now in a secured location.
b. An inventory of the prescription pad stock and reconciliation of the pads have been conducted and will continue to be performed periodically.

ATHLETICS MEDICINE

GOVERNANCE

Recommendation 5

We recommend that the campus:
a. Document the relationship between SHS and athletics, including the roles, responsibilities, reporting structure, athletics medicine director’s accountability to the medical director at SHS, and funding arrangements.

b. Obtain written designation from the president or designee of the physician responsible for medical oversight of the athletics medicine program.

c. Document who is responsible for the direct supervision of the consulting physicians who are working for athletics medicine but are not part of the SDSM arrangement.

d. Update the scope of services policy to clarify the role of the SHS medical director in athletics medicine.

Campus Response

We concur.

a. The campus will document the relationship between SHS and athletics as outlined by July 1, 2014.

b. The campus will obtain written designation from the president or designee of the physician responsible for medical oversight of the athletics medicine program by July 1, 2014.

c. The campus will document who is responsible for the direct supervision of the consulting physicians who are working for athletics medicine but are not part of the SDSM arrangement by July 1, 2014.

d. The campus will update the scope of services policy to clarify the role of the SHS medical director in athletics medicine by July 1, 2014.

SCOPE OF SERVICES PROTOCOL

Recommendation 6

We recommend that the campus review the scope of services protocol for athletics medicine biennially.

Campus Response

We concur. The campus will review the scope of services protocol for athletics medicine biennially. The first review will be completed by July 1, 2014.

PHARMACY POLICIES

Recommendation 7

We recommend the campus update athletics pharmacy policies to include:

a. Provisions for formal inventory procedures that compare expected stock to actual stock and record and account for variances.
b. A written protocol that describes the removal and disposal of outdated, deteriorated, or recalled medications.

c. A policy describing the practice for inspecting travel kits and maintaining a log documenting such inspections.

Campus Response

We concur.

a. The campus will establish formal inventory procedures that compare expected stock to actual stock and record and account for variances. This will be completed by April 30, 2014.

b. The campus will establish a written protocol that describes the removal and disposal of outdated, deteriorated, or recalled medications. This will be completed by April 30, 2014.

c. The campus will establish a policy describing the practice for inspecting travel kits and maintaining a log documenting such inspections. This will be completed by April 30, 2014.

PHARMACY

Recommendation 8

We recommend the campus update its policy for pharmaceutical requests to address the requirement that formulary content be reviewed at least annually and name the person who will perform the review, and finalize the policy.

Campus Response

We concur. The campus will update its policy to include the requirement to review formulary content at least annually, to identify the person who will perform the review, and to finalize the policy. This will be completed by April 30, 2014.

INFORMATION AND DATA SECURITY

INFORMATION SECURITY AWARENESS TRAINING

Recommendation 9

We recommend that the campus train all employees with access to protected data in information security awareness.

Campus Response

We concur. The campus will train all SHS employees with access to protected data in information security awareness by April 30, 2014.
NETWORK SEGMENTATION

Recommendation 10

We recommend that the campus place SHS servers containing protected data on a separate network segment from user computers.

Campus Response

We concur. The campus is implementing a plan to separate the servers and user computers into separate network segments, and will accept the associated risks until implementation is completed.

ENCRYPTION

Recommendation 11

We recommend that the campus encrypt sensitive data maintained in the electronic medical records and dental systems.

Campus Response

We concur. The campus is implementing a plan to work with vendors and upgrade the systems to encrypt sensitive medical and dental system records, and will accept the associated risks until implementation is completed.

VULNERABILITY MANAGEMENT

Recommendation 12

We recommend that the campus perform periodic vulnerability scans of SHS servers connected to the campus network.

Campus Response

We concur. The campus will perform, by July 1, 2014, periodic vulnerability scans of SHS servers connected to the campus network.

SYSTEM ACCESS CONTROLS

Recommendation 13

We recommend that the campus:

a. Maintain a complete inventory of user accounts with privileged access.

b. Perform periodic, documented management reviews of privileged and user accounts within all systems containing protected data.

c. Restrict access to protected information in the electronic medical records and dental systems to individuals on a need-to-know basis.
Campus Response

We concur.

a. The campus will maintain a complete inventory of user accounts with privileged access by April 30, 2014.

b. The campus will perform periodic, documented management reviews of privileged and user accounts within all systems containing protected data. This will be completed by April 30, 2014.

c. The campus will restrict access to protected information in the electronic medical records and dental systems to individuals on a need-to-know basis. This will be completed by April 30, 2014.

DISASTER RECOVERY PLAN

Recommendation 14

We recommend that the campus develop a written IT DRP for SHS computer systems.

Campus Response

We concur. The campus will develop the IT DRP by July 1, 2014.
March 4, 2014

MEMORANDUM

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

FROM: Timothy P. White  
Chancellor

SUBJECT: Draft Final Report 13-60 on Student Health Services,  
San Diego State University

In response to your memorandum of March 4, 2014, I accept the response as submitted with the draft final report on Student Health Services, San Diego State University.

TPW/amd