HIPAA COMPLIANCE

CALIFORNIA STATE UNIVERSITY,
LOS ANGELES

Audit Report 10-52
October 29, 2010

Members, Committee on Audit

Henry Mendoza, Chair
Raymond W. Holdsworth, Vice Chair
Nicole M. Anderson  Margaret Fortune
George G. Gowgani  Melinda Guzman
William Hauck

Staff

University Auditor: Larry Mandel
Senior Director: Michelle Schlack
Audit Manager: Michael Zachary
Senior Auditor: Wendee Shinsato

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
APPENDICES

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

ABBREVIATIONS

CSU California State University
EAP Employee Assistance Program
HHS U.S. Department of Health & Human Services
HIPAA Health Insurance Portability and Accountability Act
HITECH Act Health Information Technology for Economic and Clinical Health Act
HR Human Resources
PHI Protected Health Information
Privacy Rule Standards for Privacy of Individually Identifiable Health Information
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2009, the Board of Trustees, at its January 2010 meeting, directed that Health Insurance Portability and Accountability Act (HIPAA) compliance be reviewed.

We visited the California State University, Los Angeles campus from June 28, 2010, through July 8, 2010, and audited the procedures in effect at that time.

Our study and evaluation did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on HIPAA compliance activities. However, we did identify other reportable weaknesses that are described in the executive summary and body of this report. In our opinion, the operational and administrative controls for HIPAA compliance activities in effect as of July 8, 2010, taken as a whole, were sufficient to meet the objectives stated in the “Purpose” section of this report.

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 [6]

The privacy/business associate agreement with a service provider who had access to protected health information (PHI) was not entered into in a timely manner.

TRAINING [6]

Training for employees who had access to PHI was not documented.
INTRODUCTION

BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was issued by the U.S. Department of Health & Human Services (HHS). California State University (CSU) campuses and the Office of the Chancellor must comply with HIPAA by adhering to federal statutes regarding security and confidentiality of sensitive medical records maintained by the CSU entity and its business units.

HHS issued the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) to implement the requirements of HIPAA. The Privacy Rule took effect on April 14, 2003, with a one-year extension for certain “small plans,” and established a set of national standards for the protection of certain health information. Those standards address the use and disclosure of individuals’ protected health information (PHI) by covered entities, as well as individuals’ right to understand and control how their health information is used. Given that the health-care marketplace is diverse, the Privacy Rule is designed to be flexible and comprehensive so it can cover the variety of uses and disclosures that need to be addressed, and so it does not block the flow of information health-care providers need to provide high-quality care and protect the public health. The HHS Office for Civil Rights is responsible for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil monetary penalties.

As part of the American Recovery and Reinvestment Act of 2009, Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) was enacted to address the privacy and security concerns associated with the electronic transmission of health information. The HITECH Act extends the privacy and security provisions of HIPAA, including newly updated civil and criminal penalties, to business associates of covered entities, and it identifies the allocation of responsibility for the shared business associate and covered entity liability with regard to breach of the HITECH Act. Subtitle D of the HITECH Act also establishes new notification requirements for covered entities, business associates, vendors of personal health records, and related entities in the event a breach of PHI occurs. These changes are required in all business associate agreements with covered entities. The regulations associated with the new enhancements to HIPAA enforcement took effect on November 30, 2009.

Historically, CSU compliance with privacy regulations became effective April 14, 2003, according to Title II regulations. The CSU responded to HIPAA legislation by developing its own policies to ensure adequate compliance. These included the CSU HIPAA Privacy Summary Manual, Executive Order 877, and Human Resources (HR) Coded Memorandum HR 2003-14 (later superseded by HR 2004-22), all of which were issued in 2003.

HIPAA Title II requirements cover the privacy and security of individual health information used, transmitted, and retained by employer health plans and other covered entities, and the electronic transmission of PHI. The HIPAA rules that the CSU must abide by include:

- Privacy rules that safeguard the privacy of individual health information by placing limits on the accessibility and dissemination of patient information.
- Electronic data interchange rules that standardize transactions/code sets for electronic data interchange in order to encourage electronic commerce in health care.

- Security rules that maintain confidentiality and data integrity, prevent unauthorized use of data, and guard against physical hazards.

The privacy regulations affect almost every employer that sponsors a health plan. If an entity creates, maintains, or receives PHI other than enrollment, disenrollment, premium payment information, or summary health information, it must comply with HIPAA regulations. Health-care providers who transmit health information in electronic form in connection with specific types of transactions are also subject to HIPAA. The CSU self-identifies its covered components, which include many campus benefits offices and student health centers. In addition, CSU-sponsored health benefit plans, including the health-care reimbursement account plan and the campus-sponsored external employee assistance programs, are subject to HIPAA privacy regulations.
Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to HIPAA compliance and to determine the adequacy of internal 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 HIPAA compliance incorporates a defined mission, stated goals and objectives, and clear lines of organizational authority and responsibility.
- Policies and procedures are current and comprehensive, and distribution procedures are effective.
- Health-care components have been properly designated.
- A privacy official and privacy contacts have been appointed to deal with HIPAA policies and compliance.
- Business associates safeguard PHI and have signed appropriate contracts and confidentiality agreements.
- Document-retention procedures are in place to ensure that sensitive HIPAA information is maintained in accordance with regulations.
- Notices of privacy practices for PHI have been appropriately distributed, and privacy notification procedures are in place.
- Disclosure of PHI is controlled by proper consent and authorization documents and verbiage.
- Procedures allow individuals to receive communication of PHI through alternate means or at alternate locations, different from typical methods of transmission.
- Procedures are in place to protect against inappropriate disclosures of PHI, and reporting procedures exist should a breach occur.
- Health-care components have performed risk assessments sufficient to identify risks and vulnerabilities to electronic PHI.
- Sufficient HIPAA-related training has been provided to both new and established employees.
SCOPE AND METHODOLOGY

The proposed scope of the audit as presented in Attachment B, Audit Agenda Item 2 of the January 26 and 27, 2010, meeting of the Committee on Audit stated that HIPAA compliance includes review of compliance with federal statutes regarding security and confidentiality of sensitive medical records maintained by the campus. Proposed audit scope would include review of Trustee policy, federal directives, systemwide directives, and campus policies and procedures; procedures for handling confidential information; communications; training; and necessary retention of key 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 January 1, 2008, through June 30, 2010.

A preliminary risk assessment of campus HIPAA compliance information was used to select for our audit testing those areas or activities with highest risk. This assessment was based upon a systematic process using management’s feedback and professional judgments on probable adverse conditions and other pertinent information, including prior audit history in this area. We sought to assign higher review priorities to activities with higher risks. As a result, not all risks identified were included within the scope of our review.

Based upon this assessment of risks, we specifically included within the scope of our review the following:

- Evaluation of campus HIPAA organization and health-care components.
- Business associate contracts and agreements and the related confidentiality of PHI handling.
- HIPAA privacy notice procedures.
- Safeguards in place to control PHI.
- Authorization documents necessary to use and/or disclose PHI.
- Reporting procedures in place in the event of a breach of PHI.
- Campus risk assessment procedures for health-care components.
- Recordkeeping and document-retention procedures sufficient to comply with regulations.
- HIPAA-related training and continuing education for both new and established employees.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

PROGRAM ADMINISTRATION

The privacy/business associate agreement with a service provider who had access to protected health information (PHI) was not entered into in a timely manner.

We found that although there had been a contract in place since 1999 with Community Action/EAP, the external employee assistance program (EAP) provider, a privacy/business associate agreement was not entered into until April 2010.

The California State University (CSU) Health Insurance Portability and Accountability Act (HIPAA) Privacy Summary Manual, Privacy/Business Associate Agreements, §8.03, states that the CSU has determined that external EAP vendors are business associates and that the plan will require each business associate to sign a privacy/business associate agreement. Campus privacy contacts will be responsible for obtaining a privacy agreement from the external EAPs.

The HIPAA of 1996, Business Associate Contracts, §164.504(e), provides standards on the required components of a business associate contract.

The manager of compensation/classification and benefits stated that the contract with Community Action/EAP contained confidentiality language and that she was unaware that a privacy/business associate agreement was also required.

Failure to maintain appropriate privacy/business associate agreements with HIPAA partners increases the risk of misunderstandings and potential legal liabilities.

Recommendation 1

We recommend that the campus ensure that privacy/business associate agreements are entered into at the inception of any future contracts with service providers who have access to PHI.

Campus Response

We concur. Procedures regarding maintaining proper privacy/business associate agreements were reiterated to staff in November 2010.

TRAINING

Training for employees who had access to PHI was not documented.

We noted that although the campus stated that HIPAA training was provided to benefits staff who had access to PHI, this training was not documented.
The CSU HIPAA Privacy Summary Manual, *Training*, §7.02, states that workforce members of CSU who will have access to PHI will receive privacy training. It further states that the campus privacy contacts will coordinate the training for each CSU campus and that documentation of privacy training will be maintained for at least six years from the date of its creation or date when it was last in effect, whichever is later.

The HIPAA of 1996, *Safeguards*, §164.530(b), states that a covered entity must train all members with respect to PHI and that this training must be documented in written or electronic form and retained for six years from the date of its creation or date when it was last in effect, whichever is later.

The manager of compensation/classification and benefits stated that although training has been provided for her staff, she was unaware of the requirement to document the training.

Failure to document training increases the risk of misunderstandings and potential legal liabilities.

**Recommendation 2**

We recommend that the campus ensure that all future HIPAA training is documented, including the date provided, names of attendees, and course descriptions, agendas, or other examples of the training materials.

**Campus Response**

We concur. The campus has documented staff HIPAA training sessions starting in October 2010.
## APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>James M. Rosser</td>
<td>President</td>
</tr>
<tr>
<td>Lisa Chavez</td>
<td>Vice President and Chief Financial Officer, Administration and Finance</td>
</tr>
<tr>
<td>Tanya Ho</td>
<td>University Internal Auditor</td>
</tr>
<tr>
<td>Monica Jazzabi</td>
<td>Director and Medical Chief of Staff, Student Health Center</td>
</tr>
<tr>
<td>Sheryl Okuno</td>
<td>Director, Information Technology Security and Compliance</td>
</tr>
<tr>
<td>Lisa Sanchez</td>
<td>Assistant Vice President, Human Resources Management</td>
</tr>
<tr>
<td>Susie Varela</td>
<td>Assistant Director, Human Resources Management</td>
</tr>
<tr>
<td>Nancy Wada-McKee</td>
<td>Assistant Vice President, Student Affairs</td>
</tr>
<tr>
<td>Deborah Williams</td>
<td>Manager, Compensation/Classification, Benefits</td>
</tr>
</tbody>
</table>
November 3, 2010

Mr. Larry Mandel, University Auditor
Office of the University Auditor
Office of the Chancellor – The California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4210

Re: University’s Response to Recommendations Contained in Report Number 10-52
HIPAA Compliance

Dear Mr. Mandel:

Attached are the University’s responses to the recommendations contained in Report Number 10-52, Health Insurance Portability and Accountability Act (HIPAA) compliance.

Please contact Tanya Ho, University Internal Auditor, at (323) 343-5102, if you wish to discuss any matter contained herein.

Sincerely,

James M. Rosser
President

Attachment

cc: (with attachments)
Lisa Chavez, Vice-President for Administration and Chief Financial Officer
Tanya Ho, University Internal Auditor
Jill Carnahan, Administrative Compliance Officer
HIPAA COMPLIANCE

CALIFORNIA STATE UNIVERSITY,
LOS ANGELES

Audit Report 10-52

PROGRAM ADMINISTRATION

Recommendation 1

We recommend that the campus ensure that privacy/business associate agreements are entered into at the inception of any future contracts with service providers who have access to PHI.

Campus Response

Procedures regarding maintaining proper privacy/business associate agreements were reiterated to staff in November 2010.

TRAINING

Recommendation 2

We recommend that the campus ensure that all future HIPAA training is documented, including the date provided, names of attendees, and course descriptions, agendas, or other examples of the training materials.

Campus Response

The campus has documented staff HIPAA training sessions starting October 2010.
November 24, 2010

MEMORANDUM

TO: Mr. Larry Mandel  
   University Auditor

FROM: Charles B. Reed  
       Chancellor

SUBJECT: Draft Final Report 10-52 on HIPAA Compliance,  
         California State University, Los Angeles

In response to your memorandum of November 24, 2010, I accept the response  
as submitted with the draft final report on HIPAA Compliance, California State  
University, Los Angeles.

CBR/amd