

HIPAA COMPLIANCE
CALIFORNIA STATE UNIVERSITY,
EAST BAY

Audit Report 10-53
October 25, 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: Linda Rathfelder

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction.....	2
Background	2
Purpose.....	4
Scope and Methodology.....	5

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Program Administration.....	6
-----------------------------	---

APPENDICES

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

ABBREVIATIONS

CFR	Code of Federal Regulations
CSU	California State University
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	<i>Standards for Privacy of Individually Identifiable Health Information</i>
SHCSC	Student Health and Counseling Services Center

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, East Bay campus from July 26, 2010, through August 6, 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 August 6, 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 Health Insurance Portability and Accountability Act (HIPAA) security and privacy manuals at the student health and counseling services center (SHCSC) were not periodically reviewed or updated.

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.

PURPOSE

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 established to comply with regulations.
- ▶ HIPAA-related training and continuing education for both new and established employees.

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

PROGRAM ADMINISTRATION

The Health Insurance Portability and Accountability Act (HIPAA) security and privacy manuals at the Student Health and Counseling Services Center (SHCSC) were not periodically reviewed or updated.

We noted that the SHCSC's manuals, which documented policies and procedures established to ensure compliance with HIPAA regulations, had not been reviewed or updated since 2005. Specifically:

- ▶ The inventory of electronic protected health information (PHI) included discontinued software and obsolete hardware such as floppy disks.
- ▶ The security officer's job description and duties were inaccurate. For example, they included responsibility for system backup and disaster recovery; however, the security officer could not perform those duties because the servers were no longer located in the SHCSC facility.
- ▶ The servers had been moved to the campus information and computing services facility, prompting changes to security and backup procedures, but these changes were not documented.

Code of Federal Regulations (CFR) Title 45, *Security Standards: Maintenance*, §164.306(e), states that security measures implemented to comply with standards and implementation specifications adopted under §164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic PHI as described at §164.316.

45 CFR, *Standards: Documentation*, §164.316(b), states that a covered entity must maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form and review documentation periodically, and update as needed in response to environmental or operational changes affecting the security of the electronic PHI.

State Administrative Manual §20050 states that policy and procedural or operational manuals that are either not currently maintained or are non-existent could be indicative of a poorly maintained or vulnerable control system.

The medical director of student health and counseling services stated that failure to update the HIPAA security and privacy manuals to reflect present/actual clinic practices was due to oversight.

Failure to review and update policies and procedures may cause misunderstandings and potential legal liabilities.

Recommendation 1

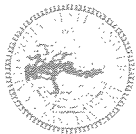
We recommend that the campus ensure that HIPAA security and privacy manuals are periodically reviewed and updated at the SHCSC.

Campus Response

We concur. Student Health and Counseling Services will continue to maintain and update the HIPAA privacy policy and procedure manual annually, beginning January 3, 2011.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Mohammad Qayoumi	President
Shawn Bibb	Vice President, Administration and Finance
Jim Cimino	Associate Vice President, Human Resources
Thomas Dixon	Network Security Analyst
Gail Erickson	Health Records Technician, Student Health and Counseling Services
Diane George	Information Technology Consultant
Mark Khoo	Medical Director, Student Health and Counseling Services
Karen Reynolds	Benefit Programs Specialist, Human Resources
Flora Salas	Administrative Analyst, Student Health and Counseling Services



CALIFORNIA STATE
UNIVERSITY
E A S T B A Y

Office of the Vice President, Administration
and Finance & Chief Financial Officer

CALIFORNIA STATE UNIVERSITY, EAST BAY
25800 Carlos Bee Boulevard, Hayward, CA 94542-3002
510.885.3803 • 510.885.4745 (fax) • www.csueastbay.edu

RECEIVED
UNIVERSITY AUDITOR

DEC 2 - 2010

THE CALIFORNIA STATE
UNIVERSITY

November 30, 2010

Mr. Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802

**RE: Campus Responses to Recommendations: Audit Report Number 10-53
HIPAA Compliance, California State University, East Bay**

Dear Mr. Mandel, *Larry*

Enclosed is our response to the recommendation in Audit Report Number 10-53, HIPAA Compliance Audit, at California State University, East Bay.

Upon acceptance of our response, we will follow up with your office, providing supporting documentation for the recommendation.

Please let us know if you have any questions or need additional information.

Sincerely,

Shawn Bibb
Vice President, Administration & Finance, CFO

SB/ad

cc: Mohammad H. Qayoumi, President
Andrea Wilson, Director, Student Health & Counseling Services

HIPAA COMPLIANCE
CALIFORNIA STATE UNIVERSITY,
EAST BAY

Audit Report 10-53

PROGRAM ADMINISTRATION

Recommendation 1

We recommend that the campus ensure that HIPAA security and privacy manuals are periodically reviewed and updated at the SHCSC.

Campus Response

We concur.

Student Health and Counseling Services will continue to maintain and update the HIPAA privacy policy and procedure manual annually, beginning, January 3, 2011.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

CHANNEL ISLANDS

December 15, 2010

CHICO

MEMORANDUM

DOMINGUEZ HILLS

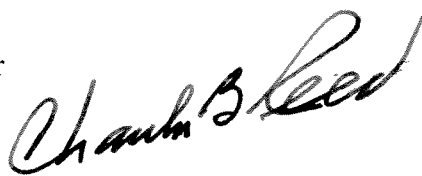
EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FULLERTON

FROM: Charles B. Reed
Chancellor



HUMBOLDT

SUBJECT: Draft Final Report 10-53 on *HIPAA Compliance*,
California State University, East Bay

LONG BEACH

LOS ANGELES

In response to your memorandum of December 15, 2010, I accept the response as submitted with the draft final report on *HIPAA Compliance*, California State University, East Bay.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/amd

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS