CONTENTS

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

Introduction .......................................................................................................................................................... 2
  Background ..................................................................................................................................................... 2
  Purpose ......................................................................................................................................................... 4
  Scope and Methodology ............................................................................................................................. 5

OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

General Control Environment ............................................................................................................................... 6
  Systemwide Policies and Procedures ........................................................................................................... 6
  Programmatic Responsibilities and Ownership for HIPAA ........................................................................... 6
APPENDICES

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

ABBREVIATIONS

CO Office of the Chancellor
CSU California State University
EO Executive Order
HHS 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
OGC Office of General Counsel
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. The Office of the University Auditor has never reviewed HIPAA compliance as a subject audit.

We visited five campuses from June 21, 2010, through October 8, 2010, and audited the procedures in effect at that time. Campus-specific findings and recommendations have been discussed and reported individually.

Our study and evaluation revealed certain conditions that, in our opinion, could result in significant errors and irregularities if not corrected. Specifically, the Office of the Chancellor (CO) did not maintain adequate internal control over systemwide policies and procedures and programmatic responsibilities and ownership for HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH Act) compliance. These conditions, along with other weaknesses, are described in the executive summary and body of this report. In our opinion, except for the effect of the weaknesses described above, the operational and administrative controls for HIPAA compliance activities in effect as of October 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.

GENERAL CONTROL ENVIRONMENT [6]

Systemwide policies for HIPAA compliance needed improvement. Specifically, the designated California State University health-care components listed in Executive Order 877, Attachment 1, were not current. Additionally, programmatic responsibilities and ownership for HIPAA and HITECH Act compliance, including responsibility for the development and implementation of information security and technical policies, had not been clearly defined or documented in systemwide policies.
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.
INTRODUCTION

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 audits 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.

During the course of the audit, we visited five campuses: Channel Islands, Dominguez Hills, East Bay, Fresno, and Los Angeles. We interviewed campus personnel and audited procedures in effect at the time of audit.
GENERAL CONTROL ENVIRONMENT

SYSTEMWIDE POLICIES AND PROCEDURES

Systemwide policies and procedures for Health Insurance Portability and Accountability Act (HIPAA) compliance needed improvement.

Specifically, we found that the designated California State University (CSU) health-care components listed in Executive Order (EO) 877, Attachment 1, were not current.

EO 877, Designation of Health Care Components for Purposes of the Health Care Portability and Accountability Act of 1996, dated August 5, 2003, states that the assistant vice chancellor of student academic support shall be responsible for promptly updating Attachment 1 of EO 877 to reflect all newly designated or de-designated CSU health-care components and shall append each revised version of the attachment to the EO. Each revised version of Attachment 1 shall show the effective date of the revision. A copy of each version of Attachment 1 shall be maintained for at least six years after the date it was last in effect.

The associate director for student programs, student academic support, academic affairs, stated that EO 877 was being reviewed, but Attachment 1, showing designated health-care components, was not updated due to time constraints involving the coordination of multiple reviews of health-care components in various departments and locations.

Failure to maintain written designation of current health-care components increases the risk of regulatory sanctions.

Recommendation 1

We recommend that the Office of the Chancellor (CO) update EO 877, Attachment 1, to show the current list of designated CSU health-care components.

Management Response

We concur. The CO will update EO 877 to show the current list of designated CSU health-care components. The target date for updating the EO is October 1, 2011.

PROGRAMMATIC RESPONSIBILITIES AND OWNERSHIP FOR HIPAA

Programmatic responsibilities and ownership for HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH Act) compliance, including responsibility for the development and implementation of information security and technical policies, had not been clearly defined or documented in systemwide policies.
Code of Federal Regulations Title 45, §164.308, Administrative Safeguards, specifies that a covered entity (the CSU) must implement policies and procedures to prevent, detect, contain, and correct security violations, including, but not limited to, risk analysis, risk management, sanction policies, information system activity reviews, and the assignment of a security official who is responsible for the development and implementation of the policies and procedures required by the covered entity.

Government Code §13402 and §13403 state that management is responsible for establishing and maintaining a system of internal administrative controls, which includes documenting the system, communicating system requirements to employees, and assuring that the system is functioning as prescribed and is modified, as appropriate, for changes in conditions. Further, administrative controls are the methods through which reasonable assurance can be given that measures adopted by state agency heads to safeguard assets and promote operational efficiency are being followed.

The assistant vice chancellor, systemwide human resources (HR), stated that all of the above has been duly documented and communicated to employees. She further stated that the new HITECH regulations will require a change in HIPAA oversight at the CSU. She also stated that the systemwide HIPAA policy for HR-related disclosures is being reviewed and will be revised to include requirements from the HITECH Act. The senior director of information security management stated that the CSU systemwide information security policy addresses the general requirements in the federal HIPAA regulation and that the systemwide HIPAA policy standard is being revised to include requirements from the HITECH Act.

Failure to assign programmatic responsibility for HIPAA and HITECH Act compliance, including responsibility for the development and implementation of information security and technical policies, increases the risk of misunderstandings related to the performance of duties and functions, inconsistencies in complying with state and federal requirements, inconsistent treatment and handling of issues, and possible litigation and regulatory sanctions.

**Recommendation 2**

We recommend that the CO define programmatic responsibilities and ownership for HIPAA and HITECH Act compliance, including responsibility for the development and implementation of information security and technical policies, and document them in systemwide policies.

**Management Response**

We concur. The CO will identify systemwide HIPAA privacy and security officials. These individuals will work collaboratively to manage the CSU HIPAA/HITECH compliance program and develop systemwide policies governing HIPAA and HITECH. The target date for identifying the systemwide privacy and security officials is October 1, 2011.
## APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office of the Chancellor</strong></td>
<td></td>
</tr>
<tr>
<td>Benjamin F. Quillian</td>
<td>Executive Vice Chancellor and Chief Financial Officer</td>
</tr>
<tr>
<td>George Ashkar</td>
<td>Assistant Vice Chancellor/Controller, Financial Services</td>
</tr>
<tr>
<td>James Blackburn</td>
<td>Interim Assistant Vice Chancellor, Student Academic Support, Academic Affairs,</td>
</tr>
<tr>
<td>Gail Brooks</td>
<td>Vice Chancellor, Systemwide Human Resources (HR)</td>
</tr>
<tr>
<td>Pamela Chapin</td>
<td>Director, Benefits and HR Programs</td>
</tr>
<tr>
<td>Michelle Hamilton</td>
<td>Manager, Benefits and HR Programs</td>
</tr>
<tr>
<td>Christine Helwick</td>
<td>General Counsel, Office of General Counsel (OGC)</td>
</tr>
<tr>
<td>Allison G. Jones</td>
<td>Assistant Vice Chancellor, Student Academic Support, Academic Affairs (at time of audit)</td>
</tr>
<tr>
<td>Ray Murillo</td>
<td>Associate Director, for Student Programs, Student Academic Support, Academic Affairs</td>
</tr>
<tr>
<td>Evelyn Nazario</td>
<td>Assistant Vice Chancellor, Systemwide HR</td>
</tr>
<tr>
<td>Cheryl Washington</td>
<td>Senior Director, Information Security Management, Information Security</td>
</tr>
</tbody>
</table>

**California State University, Channel Islands**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richard R. Rush</td>
<td>President</td>
</tr>
<tr>
<td>Joanne Coville</td>
<td>Vice President of Finance and Administration (At time of review)</td>
</tr>
<tr>
<td>Diana Enos</td>
<td>Human Resources Manager</td>
</tr>
<tr>
<td>Deborah Gravelle</td>
<td>Director, Leadership, Career, and Health Office</td>
</tr>
<tr>
<td>Edwin Lebiodia</td>
<td>Associate Vice President of Student Affairs</td>
</tr>
<tr>
<td>Justin Magruder</td>
<td>Administrator, Moorpark Family Medical Care Clinic</td>
</tr>
<tr>
<td>Anna Pavin</td>
<td>Interim Associate Vice President of Human Resources</td>
</tr>
</tbody>
</table>

**California State University, Dominguez Hills**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mildred Garcia</td>
<td>President</td>
</tr>
<tr>
<td>Brian Cummins</td>
<td>Manager, Benefits, Human Resources Management</td>
</tr>
<tr>
<td>Janie Macharg</td>
<td>Director, Student Health &amp; Psychological Services</td>
</tr>
<tr>
<td>Andy McDaniel</td>
<td>Business Process Management, Administration and Finance</td>
</tr>
<tr>
<td>Mary Ann Rodriguez</td>
<td>Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Mark Seigle</td>
<td>Assistant Vice President, Human Resources Management</td>
</tr>
<tr>
<td>Karen Wall</td>
<td>Associate Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Rose Welch</td>
<td>Acting Director/Associate Dean, School of Nursing</td>
</tr>
</tbody>
</table>

**California State University, East Bay**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mohammad Qayoumi</td>
<td>President (At time of review)</td>
</tr>
<tr>
<td>Shawn Bibb</td>
<td>Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Jim Cimino</td>
<td>Associate Vice President, Human Resources</td>
</tr>
<tr>
<td>Thomas Dixon</td>
<td>Network Security Analyst</td>
</tr>
<tr>
<td>Gail Erickson</td>
<td>Health Records Technician, Student Health and Counseling Services</td>
</tr>
<tr>
<td>Diane George</td>
<td>Information Technology Consultant</td>
</tr>
</tbody>
</table>
APPENDIX A: PERSONNEL CONTACTED

California State University, East Bay (cont.)
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, Fresno
John D. Welty  President
Amanda Adams  Director, Central California Autism Center
Juanita Aguilar  Benefits Manager, HR
Richard Boes  Director, Information Technology Services and Chief Information Security Officer
John Briar  Director, Campus Information Systems
Kelli Eberlein  Head Athletic Trainer, Department of Athletics
Don Freed  Chair, Communicative Disorders and Deaf Studies Department
Esther Gonzalez  Confidential Analyst, Office of the Vice President for Administration
Constance Jones  Chair, Institutional Review Board
Gary Lentell  Professor, Physical Therapy Department
John Lloyd  Director, Rehabilitation Counseling Evaluation Center
Christopher Lucey  Director, Fresno Family Counseling Center
Jan Parten  Director, HR
Nancy Petenbrink  Director, Employee Assistance and Wellness
Michael Russler  Chair, Nursing Department
Dirk Ruthrauff  Interim Director, Health and Psychological Services
Cynthia Teniente-Matson  Vice President for Administration and Chief Financial Officer
Peggy Trueblood  Chair, Physical Therapy Department
Rafael Villegas  Information Technology Security Officer

California State University, Fullerton
Monique Shay  Attorney, President’s Office and OGC HIPAA Subject-Matter Attorney

California State University, Los Angeles
James M. Rosser  President
Lisa Chavez  Vice President and Chief Financial Officer, Administration and Finance
Tanya Ho  University Internal Auditor
Monica Jazzabi  Director and Medical Chief of Staff, Student Health Center
Sheryl Okuno  Director, Information Technology Security and Compliance
Lisa Sanchez  Assistant Vice President, Human Resources Management
Susie Varela  Assistant Director, Human Resources Management
Nancy Wada-McKee  Assistant Vice President, Student Affairs
Deborah Williams  Manager, Compensation/Classification, Benefits
MEMORANDUM

DATE: June 30, 2011

TO: Larry Mandel
   University Auditor

FROM: Benjamin F. Quillian
       Executive Vice Chancellor and
       Chief Financial Officer

Ephraim P. Smith
Executive Vice Chancellor and
Chief Academic Officer

Gail Brooks
Vice Chancellor
Human Resources

SUBJECT: Management Response to Recommendations of Audit Report #10-74,
HIPPA Compliance, Systemwide

In response to the "Incomplete Draft" report dated May 25, 2011, we are providing the
enclosed management responses.

Should you have any questions, please feel free to contact any of us.

BFQ:ije

Attachment

c: Evelyn Nazario, Assistant Vice Chancellor, Human Resources Management
Cheryl Washington, Senior Director, Information Security Management
Ray Murillo, Associate Director, Student Programs
GENERAL CONTROL ENVIRONMENT

SYSTEMWIDE POLICIES AND PROCEDURES

Recommendation 1

We recommend that the Office of the Chancellor (CO) update EO 877, Attachment 1, to show the current list of designated CSU health-care components.

Management Response

We concur. The CO will update EO 877 to show the current list of designated CSU health-care components. The target date for updating the EO is October 1, 2011.

PROGRAMMATIC RESPONSIBILITIES AND OWNERSHIP FOR HIPAA

Recommendation 2

We recommend that the CO define programmatic responsibilities and ownership for HIPAA and HITECH Act compliance, including responsibility for the development and implementation of information security and technical policies, and document them in systemwide policies.

Management Response

We concur. The CO will identify systemwide HIPAA Privacy and Security officials. These individuals will work collaboratively to manage the CSU HIPAA/HITECH compliance program and develop systemwide policies governing HIPAA and HITECH. The target date for identifying the systemwide privacy and security officials is October 1, 2011.
July 13, 2011

MEMORANDUM

TO: Mr. Larry Mandel
University Auditor

FROM: Charles B. Reed
Chancellor

SUBJECT: Draft Final Report 10-74 on HIPAA Compliance, Systemwide

In response to your memorandum of July 13, 2011, I accept the response as submitted with the draft final report on HIPAA Compliance, Systemwide.

CBR/amd