The Regents of the University of California

COMMITTEE ON AUDIT
May 15, 2002

The Committee on Audit met on the above date at Covel Commons, Los Angeles campus.

Members present: Regents Davies, Marcus, Moores, Morrison, Parsky, Sayles, and Seymour

In attendance: Regents Atkinson, Blum, T. Davis, Eastin, Hopkinson, Johnson, Kozberg, Lansing, Lozano, Montoya, Pattiz, Preuss, and Saban, Regents-designate Ligot-Gordon, Sainick, and Terrazas, Faculty Representatives Binion and Viswanathan, Secretary Trivette, General Counsel Holst, Treasurer Russ, Provost King, Senior Vice Presidents Darling and Mullinix, Vice President Drake, Chancellors Bishop, Cicerone, Dynes, Greenwood, Tomlinson-Keasey, and Vanderhoef, Acting Chancellor Warren, and Recording Secretary Bryan

The meeting convened at 12:55 p.m. with Committee Chair Morrison presiding.

1. **APPROVAL OF MINUTES**

Upon motion duly made and seconded, the minutes of the meeting of March 13, 2002 were approved.

2. **ANNUAL REPORT ON THE INTERNAL AUDIT PLAN, 2002-03**

In accordance with the Schedule of Reports, the **Annual Report on the Internal Audit Plan, 2002-03** was submitted for discussion. There were no questions.

[The report was mailed in advance of the meeting, and copies are on file in the Office of the Secretary.]

3. **RESOLUTION IN SUPPORT OF UC HEALTH SCIENCES HIPAA COMPLIANCE PLAN**

The President recommended that The Regents approve the following resolution in support of the University's academic health centers' Health Insurance Portability and Accountability Act (HIPAA) Compliance Plan, an initiative of the University's Health Sciences Clinical Enterprise Corporate Compliance Program:

RESOLUTION OF THE UNIVERSITY OF CALIFORNIA BOARD OF REGENTS: ACADEMIC HEALTH CENTER INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE PROGRAM

The University's individual and institutional providers of health care recognize and respect a patient's expectations that the privacy and security of individual health information will be protected. The University is committed to implementing policies and practices that will enable it reasonably and appropriately to protect its patients' privacy while carrying out its mission of care, service, education, and research. Compliance with the mandates of The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and Security Regulations requires a thoughtful balance between the rights of the University's patients to privacy of their protected health information, the patient's expectation that high-quality care will be delivered in a cost-effective and timely manner, and society's expectation that academic health centers will continue to teach and perform leading-edge research.

The Board of Regents recognizes and supports the efforts of the members of the University's Systemwide Corporate Compliance Committee: Academic Health Center Task Force to implement a HIPAA Compliance Program that will provide for compliance by developing, where appropriate, systemwide privacy and security policies; demonstrate a commitment and leadership across the organization to the principles embodied in HIPAA; minimize disruption to the care, research, and teaching missions of the University; and enhance patient confidence in the institutions that serve them.

It was recalled that in mid-1996 the University had established the Systemwide Corporate Compliance Committee (Compliance Committee), comprised of representatives from each of the five academic health centers and the Office of the President, to implement a Universitywide effort in responding to the federal audit of the medical schools' professional fee billings, develop Professional Fee Billing Guidelines in response to new Medicare billing regulations, and provide a forum for resolution of ongoing issues related to compliance with new federal regulations. In June 1998, The Regents authorized the President to develop a Health Sciences Clinical Enterprise Corporate Compliance Program (Program) in response to scrutiny by the Department of Health and Human Services and Office of the Inspector General and demands by consumers and policy makers for increased accountability in the health care industry. The Compliance Committee was ordered to develop a program that would demonstrate the University's commitment to ethical and legal behavior in carrying out the activities of the health sciences clinical enterprise, provide specific standards of ethical and legal conduct, develop policy and practices for implementing the University's Compliance Code of Conduct, and provide annual reports to The Regents regarding the status of the program.

The Compliance Committee has identified areas of risk and has developed initiatives to enhance the overall compliance activities of the University, promote sound business practices, reduce risks of future external audits, and reduce regulatory and compliance costs for the enterprise. The Health Sciences Clinical Enterprise Corporate Compliance Annual Report (Fiscal Year 2001) provides an overview of the progress that has been made toward achieving timely compliance with HIPAA.

Compliance with the HIPAA Privacy Rule

In 2000, the Department of Health and Human Services established "Standards for Privacy of Individually Identifiable Health Information" (Privacy Rule). The Privacy Rule creates national protections for the confidentiality of the health information. Health care providers covered by the rule must comply by April 14, 2003.

The Privacy Rule requires health care providers to do the following:

- Provide information to patients about their privacy rights and how their information can be used;
- Adopt clear privacy policy and procedures for workforce members who create, access, use, and disclose protected health information;
- Educate all employees regarding privacy and security policy and procedures;
- Designate an individual to be responsible for seeing that privacy procedures are adopted and followed;
- Establish mechanisms to provide for patients to access, copy, amend, restrict, and account for the use and disclosure of their information; and
- Secure patient records so that they are available only to those who need them.

In November 2000, the Compliance Committee appointed the University's Academic Health Center HIPAA Task Force (HIPAA Task Force) in order to lead the development and implementation of a compliance business plan to accomplish the following goals:

- Reduce costs of compliance by standardizing the University's approach, creating, where appropriate, a single set of policies and practices, and sharing resources;
- Reduce the University's business and audit risks by providing consistency of approach, shared best practices, and uniform application of the Privacy Rule "reasonableness standard";
- Enhance compliance by demonstrating commitment and leadership across the organization; and
- Minimize disruption to the care, research, and teaching missions of the University.

Applicability of HIPAA Privacy Rule to the University

The Privacy Rule, as well as the security and transaction standards, covers health care providers, health plans, and health care clearinghouses. An entity that performs both covered and non-covered functions is defined as a hybrid covered entity. Most of the requirements of the Privacy Rule apply only to the health care components of the hybrid covered entity. These include workforce members who perform covered health care functions and workforce members who support those functions. The Privacy Rule requires the hybrid covered entity to define and designate the parts of the entity that engage in the covered health care provider functions and provide business associate support functions to the covered health care provider.

Covered Functions of the University's Health Care Component

The HIPAA Taskforce recommends that The Regents designate the University of California as a hybrid covered entity with a single health care component that includes but is not limited to the following:

- The five University academic health centers, including their medical centers and clinics and Schools of Medicine, Dentistry, Pharmacy, Nursing, Optometry, and Public Health;
- University of California at Berkeley School of Public Health;
- Student Health Centers;
- Employee-assistance and/or employee health services;
- Clinical research sites; and
- Pharmacies.

University Entities that Support the Covered Functions of the University's Health Care Component

The HIPAA Taskforce recommends that those entities within the University that support those covered functions of the hybrid entity and, as such, would be designated as elements of the University's single health care component of the hybrid covered entity, include but not be limited to the following:

- University Office of the President divisions: General Counsel; University Auditor; Clinical Services Development; Health Affairs; System Corporate Compliance Committee and HIPAA Taskforce; Research; Risk Management, Human Resources and Benefits, and Third Party Administrators; and IT Security.

- Campus offices and divisions with operational responsibility comparable to those listed within the Office of the President as well as Institutional Review Boards; ombudsman; student field placements; the Division of Health and Safety; and Clinical Engineering.

Separating the Health Care Component

The Privacy Rule requires the University to create adequate separation between its single health care component and all other components. Transfer of protected health information by the University's health care component to other components of the hybrid covered entity is considered a disclosure under the Privacy Rule and is allowed only to the same extent as such disclosure would be permitted to a separate entity. Failure to comply with the Privacy Rule requirements for use and disclosure of protected health information within the University may result in civil or criminal liabilities.

As a step toward meeting the April 2003 compliance deadline, the HIPAA Task Force, in coordination with the Office of the General Counsel, the University Auditor, and the Office of Business and Finance, has developed a compliance business plan that determines the applicability of HIPAA to the operational units within the University.

Security of Data

Although the Department of Health and Human Services has not published the final HIPAA security rule, the Task Force intends to implement a Security Business Plan to address the following five proposed security components:

- Administrative procedures with documented security policies, procedures, and practices intended to maintain data integrity, ensure confidentiality, and make health information available to those who need it. Requirements under this area include contingency plans for system emergencies, policies on access control, protection of data, partner agreements for all trading partners who exchange protected health information, and training for all employees and agents regarding security;
- Physical safeguards requiring controls and security for physical facilities, computer systems, and associated equipment;
- Technical security services designed to protect, control, and monitor information access, such as access control, audit controls, consent for use and disclosure, data authentication, and user identification;
- Technical security mechanisms that include processes created for preventing unauthorized access, integrity controls, and message authentication for data that are sent over a network; and
- Electronic signature that includes recommendations for but does not require the use of electronic signatures for any of the HIPAA transactions.

Achieving compliance with the Privacy Rule requires the implementation of security standards. The failure to finalize the security standards could force providers to incur additional regulatory burdens as they attempt to comply with privacy requirements without a full understanding of the final security requirements.

Upon motion duly made and seconded, the Committee approved the President's recommendation and voted to present it to the Board.

The meeting adjourned at 12:57 p.m.

Attest:

Secretary