

The Regents of the University of California

**COMMITTEE ON AUDIT
COMMITTEE ON HEALTH SERVICES**

May 14, 2003

The Committees on Audit and Health Services met jointly on the above date at UCSF–Laurel Heights, San Francisco.

Members present: Representing the Committee on Audit: Regents Connerly, Hopkinson, Lee, Lozano, Moores, and Terrazas; Advisory member Binion
Representing the Committee on Health Services: Regents Davies, Johnson, Kozberg, Lee, Moores, Preuss, Sainick, Sayles, and Terrazas; Advisory members Seigler and Pitts

In attendance: Regents Ligot-Gordon, Marcus, and Montoya, Regent-designate Murray, Associate Secretary Shaw, General Counsel Holst, Treasurer Russ, Provost King, Senior Vice Presidents Darling and Mullinix, Vice Presidents Broome, Doby, Drake, Gurtner, and Hershman, Chancellors Berdahl, Cicerone, Córdova, Dynes, Vanderhoef, and Yang, Vice Chancellor Desrochers representing Chancellor Tomlinson-Keasey, and Recording Secretary Bryan

The meeting convened at 11:00 a.m. with Committee on Health Services Chair Lee presiding.

UC COMPLIANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Senior Vice President Mullinix recalled that the Health Insurance Portability and Accountability Act of 1996 mandated significant changes in the legal and regulatory environments governing the provision of health benefits, the delivery of and payment for healthcare services, and the security and confidentiality of individually identifiable protected health information (PHI) in written, electronic, or oral formats. Under HIPAA, the Privacy Rule provides for the privacy of an individual's health information. The Administrative Simplification Standards provide for the standardization of transactions and formats used for electronic communication of healthcare data. The Security Rule provides for the security of an individual's health information when the information is transmitted electronically.

In May 2002, the Board of Regents took action to support the recommendation of the HIPAA Task Force that all University HIPAA-covered entities would comprise a Single Health Care Component (SHCC) and would implement a system-wide approach to achieving compliance with the HIPAA Privacy Rule in order to reduce the costs and risks of compliance and to provide for a consistent interpretation of the complex requirements of the rule.

The Privacy Rule

The HIPAA Privacy Rule requires all covered entities to protect the privacy and security of an individual's PHI. The Privacy Rule also stipulates that, with some exceptions, State law will prevail when it is more protective of privacy rights than is federal law.

The Privacy Rule required all covered institutions to have met specific administrative and organizational mandates by the compliance date of April 14, 2003. For over two years, the HIPAA Task Force has been engaged in developing a consistent and comprehensive University response to the Privacy Rule. The Task Force has recently grown from a group of 20 members from the University's academic health centers, the office of the University Auditor, and the Office of the General Counsel to over 115 active participants with additional representation from the chancellor's offices at all campuses, the Division of Business and Finance, and the University's Department of Energy laboratories. Contingent on the definition of the University as a Single Health Care Component, the HIPAA Privacy Rule requires that the University document all HIPAA-covered healthcare providers, HIPAA-covered self-insured health plans, and business and finance units that provide services to the providers and health plans. The following entities and their respective workforce members are a part of the University's SHCC:

- The healthcare providers include the five academic health centers; health professional schools when they provide clinical care or training in a clinical setting; student health services at all campuses; occupational health or medical clinics at campuses and University-operated Department of Energy labs; some athletic departments and/or trainers; and behavioral health and other student, employee, or community-based clinics;
- The University's self-insured health plans;
- The University's business, financial, and legal units if they use PHI to conduct business for the HIPAA-covered providers and health plans, including the President's Immediate Office, the President's Cabinet and staff, The Regents, the Office of the Secretary of The Regents, the Office of the General Counsel, the Division of Business and Finance, the University Auditor, the Institutional Review Boards for research, and others as determined.

Additionally, the University must define those entities and workforce members who are not covered by HIPAA and are not part of the SHCC, to safeguard the flow of PHI between the SHCC and non-covered entities and workforce members.

The Privacy Rule is complicated. In areas where the law is not clear, the stated principles behind the HIPAA Privacy Rule and Office for Civil Rights' communications give covered entities some flexibility in implementing the standards. Based on extensive legal and policy analyses of the requirements of the rule and the specific application to the University's covered entities, the HIPAA Task Force has developed the HIPAA Privacy Rule System Standards (System Standards), which provide specific guidance for compliance with the rule

and flexibility to implement procedures that reflect local practice. Further, the HIPAA Task Force has developed legal documents and other model forms as required by the Privacy Rule, including the Notice(s) of Privacy Practices.

University Privacy Officer Faer has been appointed as the SHCC's Privacy Official, and a Privacy Office has been established within the Office of Business and Finance for ongoing development and monitoring of the policies and for handling complaints. At the campus level, each of the academic health centers has appointed a local Privacy Officer responsible for compliance within those covered entities, and each chancellor has appointed at least one individual to serve as Privacy Liaison to the HIPAA Task Force and to be responsible for compliance on behalf of covered entities and workforce members at the campus level. As required by the HIPAA Privacy Rule, the University has documented the responsibilities of the designated individuals and posted the information on the University's newly-established HIPAA website.

The Privacy Rule and the University's System Standards mandate that the SHCC train all HIPAA-covered workforce members on the requirements of the rule and retain documentation that the training has occurred. To provide consistency and to create economies of scale, the HIPAA Task Force developed and distributed training modules for use by all covered entities within the University, including basic training for all workforce members and additional presentations for specific audiences. In order to meet this requirement as a single system, the SHCC's privacy officers and liaisons will certify to the Privacy Official that the required training has been accomplished and documented.

The Privacy Rule requires that covered entities identify all third-party vendors and contractors who use or disclose PHI on their behalf and enter into agreements that assure the business associates will protect the information. All covered entities within the University have been working to identify those business associates and to reach consensus with contractors as to what their obligations are under the rule.

The HIPAA Task Force will provide a follow-up report to the Board no later than January 1, 2004 regarding ongoing compliance with the Privacy Rule and, in particular, compliance with the organizational and administrative mandates.

Standardization of Transactions

Under HIPAA, payers and providers must conform to a national standard for electronic maintenance and transmission of patient claims and other forms. Within the University, healthcare providers will have until October 2003 to comply with this requirement but will be dependent on HIPAA-covered clearinghouses, health plans, and software vendors outside the University's control to implement the systems and software upgrades necessary for everyone to meet the deadline of October 2003. If there are delays, the problem could be passed on to healthcare providers, and Medicare and other payers may deny claims if forms do not fit the HIPAA-required format. HIPAA Task Force members are working collaboratively to develop best practices and determine how to achieve compliance in an environment dependent on third-party software vendors and on Medicare, Medicaid, and private payers.

The Security Rule

On February 20th of this year, the Department of Health and Human Services published the final HIPAA Security Rule, with an implementation date of April 2005. The HIPAA Security Rule expects covered entities to build upon the policies and procedures developed for compliance with the HIPAA Privacy Rule. The HIPAA Task Force is working with Information Resources and Communications in the Office of the President and with campus and academic health center information officers to develop a planning process for the Security Rule similar to that used for the Privacy Rule.

The meeting adjourned at 11:05 a.m.

Attest:

Associate Secretary