California State University
HIPAA PRIVACY POLICY

The California State University's (CSU) health benefit plans must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Title II regulations, issued by the Federal Department of Health and Human Services (DHHS). How the CSU complies with the HIPAA regulations will vary with the particular health plan and the CSU's involvement in plan administration functions.

HIPAA's 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 certain individual health data. This information is known as protected health information (PHI). There are three main sets of HIPAA regulations, each part with differing effective dates.

HIPAA Regulations	Description	Effective Dates
Privacy	Rules that safeguard privacy of individual health information by placing limits on accessibility and dissemination of patient information.	April 14, 2003, unless meets "small plan rule" then April 14, 2004.
Electronic Data Interchange (EDI)	Rules that standardize transactions/code sets for electronic data interchange to encourage electronic commerce in healthcare.	October 16, 2003
Security	Rules that maintain confidentiality and data integrity, prevent unauthorized use of data, and guard against physical hazards.	April 21, 2005

Health Plan Types Subject to HIPAA's Privacy Regulations

- Major medical, pharmacy, disease-specific policies (such as cancer coverage)
- Dental, vision, long-term care, mental health
- Some Employee Assistance Programs (EAPs)
- Health Flexible Spending Accounts (FSAs)

Privacy Regulations Apply to Covered Entities and Business Associates

Covered Entities	
Health Plans	– Any plan that provides health benefits or pays for health care – Includes insured plans (CalPERS medical, Delta Dental, PMI dental, BlueShield/MES vision and external EAPs) and self-insured health plans (HCRA), HMOs, and insurers
Health Care Providers	– Applies if they transmit health data electronically – Can include on-site clinics and medical facilities
Health Care Clearinghouses	– Billing agents and firms that process electronic health information

Typically employers, third party administrators (TPAs), life insurance plans, disability plans, worker's compensation plans and agencies are not covered entities. However, HIPAA regulations make it clear that employers and their TPAs may be affected based on their roles as plan sponsors and business associates.

Business Associates
A business associate is an entity that performs functions for or provides services to or on behalf of, a covered entity, where the function or service involves the use or disclosure of individually identifiable health information. Business associates must agree via contract with a group health plan that they will comply with the HIPAA regulations. Certain entities are not business associates, including insurers and HMOs providing insured benefits, and employers performing administrative activities for their plans. Examples of business associates include: TPAs, consultants, attorneys, and auditors. The CSU must have a business associate agreement with its Health Care Reimbursement Account (HCRA) Plan TPA and a privacy agreement, similar to a business associate agreement, with all its external campus-sponsored employee assistance programs (EAPs). **COBRA** vendors may be considered business associates for purposes of HIPAA compliance. Benefit plans must ensure that there is a business associate agreement in place. This responsibility lies with the insurance carriers if they contract out their COBRA operations. CSU does not contract directly with any COBRA vendor. This is not applicable to the CSU but may be for its insurance carriers.

The Regulations Affect Employers including the CSU

HIPAA regulations affect almost every employer that sponsors a health plan, including the CSU. Although employers are not directly regulated by the HIPAA regulations, the group health benefit plans they sponsor are. The employer, as the plan administrator for a group health benefit plan, is responsible for ensuring the plan's compliance with the regulations. Employers are, generally, not "covered entities," but the privacy rules require employers that perform administrative services for their health plans to implement safeguards.

If an employer only 1) receives summary health information for limited purposes of obtaining premium bids or for modifying, amending, or terminating plans and 2) only transmits participant enrollment, disenrollment, premium payment information to the business associates, insurers, and HMOs that administer the group health benefit plan, then the employer is generally "off the HIPAA hook."

However, if the employer creates, maintains or receives protected health information (PHI) other than enrollment, disenrollment, premium payment information or summary health information, the employer is subject to more of the regulations.

Privacy Regulations – Impact on CSU

- CSU's sponsored health benefit plans (medical, dental, and vision) are subject to the HIPAA privacy regulations effective April 14, 2003. The Health Care Reimbursement Account (HCRA) plan and campus-sponsored external Employee Assistance Programs (EAPs) are subject to the regulations effective April 14, 2004.

- HIPAA does not affect CSU's treatment of health-related information that is acquired through ordinary human resources operations (i.e., campus generated enrollment and disenrollment in benefit plans, fitness for duty examinations, medical restrictions, and accommodations for disabilities) and is used for ordinary human resources operations.

- The privacy regulations do affect the scope of information that the health benefit plan providers (i.e., CalPERS medical, Delta, PMI, BlueShield/MES and external EAPs) can disclose to the CSU beyond summary health information and enrollment and disenrollment information.

- The CSU's health benefit plan insurers and HMOs are covered entities under HIPAA privacy regulations and as such must establish privacy policy and procedures, including restrictions on the use or disclosure of PHI.

- The Health Care Reimbursement Account (HCRA) plan is self-insured; therefore, the CSU, as plan sponsor, is responsible for the HCRA plan's compliance with HIPAA privacy regulations, including establishing privacy policy and procedures that restrict the use and disclosure of PHI.

- CSU staff dealing with PHI must be trained regarding HIPAA policies and procedures, safeguard PHI against intentional or accidental misuse, disclose only the minimum necessary amount of information, and are prohibited from retaliating against participants who file a complaint.

- CSU participants have the right to receive privacy notices, inspect a copy of their PHI, amend PHI, request restricted use of PHI, receive an accounting of non-routine disclosures of their PHI and file a complaint about privacy violations.

- HIPAA privacy regulations will be enforced by the Federal DHHS Office of Civil Rights through complaints and selected audits. Civil and criminal penalties can be enforced.

CSU Human Resources Specific HIPAA Privacy Materials

HIPAA Privacy Policy Manual: A campus specific HIPAA Privacy Policy Manual is available for use by campus human resources departments when dealing with HIPAA privacy regulation compliance. This manual will be available for viewing online at the HIPAA web site in the near future. The URL will be provided under separate cover.

CSU Multi Benefit Plan HIPAA Privacy Notice: Newly benefits eligible employees are to be provided with the CSU multi benefit plan HIPAA Privacy Notice. This notice covers CSU sponsored health benefit plans subject to HIPAA privacy regulations.

HIPAA Participant Authorization Form: A Participant Authorization form is to be used when an employee's authorization is needed by the campus to use PHI for purposes deemed necessary by HIPAA privacy regulations. This form can be viewed by clicking onto the following URL: http://www.calstate.edu/HRAdm/pdf2004/HR2004-22_Authorization_Form.pdf.