CSU The 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 (HHS), as amended by The Health Information Technology for Economic and Clinical Health (HITECH) Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act (ARRA) of 2009). The HITECH Act augments HIPAA's privacy and security related components, and is an expansion of HIPAA rules and obligations. These regulations intertwine to ensure that the appropriate protocols are followed regarding the protection of data and breach notifications to avoid exposure for potential fines. How the CSU complies with HIPAA and HITECH regulations will vary by health plan type and the CSU's involvement in plan administration functions.

HIPAA's Title II "administrative simplification" 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). The HITECH Act:

1) Applies the same HIPAA privacy and security requirements (and penalties) for covered entities to business associates, and mandates that the new security requirements be incorporated into all Business Associate contracts;
2) Requires HHS to conduct compliance audits in conjunction with stringent enforcement of HIPAA compliance by the HHS Office of Civil Rights;
3) Establishes mandatory federal privacy and security breach reporting requirements for entities subject to HIPAA, including business associates;
4) Requires security breaches to be reported to the media, depending on the number of impacted individuals;
5) Dramatically increases HIPAA-related penalties that were previously limited to $100 - $25,000. They now range from a minimum of $100 to $50,000 per day of violation, with an annual cap of $1.5 million for the same violation in any one year.
6) Establishes criminal penalties that are applicable to individuals, not just the entity in violation. In cases of "knowing misuse," criminal penalties include monetary fines of $50,000 up to $250,000, and imprisonment of one (1) to ten (10) years.

There are now four (4) main sets of HIPAA regulations, each part with differing effective dates.

HIPAA Regulations	Description	The HITECH ACT
Privacy	Rules that safeguard privacy of individual health information by placing limits on accessibility and dissemination of patient information.	The HITECH Act is layered over HIPAA Privacy and Security, and also expands the scope of privacy and security protections available under HIPAA. It also increases the potential legal liability for non-compliance; and it provides for increased enforcement.
Electronic Data Interchange (EDI)	Rules that standardize transactions/code sets for electronic data interchange 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.	

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 PPO, DeltaCare USA, Vision Service Plan (VSP), external Employee Assistance Programs (EAPs), 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 – Includes applicable CSU Student Health Centers
Health Care Clearinghouses	– Billing agents and firms that process electronic health information

Typically employers, third party administrators (TPAs), life insurance plans, disability plans, workers' 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). If a campus replaces its EAP provider, a signed copy of the CSU HIPAA Privacy and Business Associate Agreement must be forwarded to the CSU HIPAA Privacy Official, within Human Resources Management (HRM) in the Chancellor's Office.

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 and adhere to 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 essentially, the employer's HIPAA exposure is minimized.

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, and should exercise extreme caution regarding access, storage and destruction of such information.

HIPAA Privacy Regulations – Impact on CSU

The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information (PHI), including individual medical records and sets limits and conditions on the uses and disclosures that may be made of such information. The Privacy Rule also gives individuals rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

PHI is health information that is created, received, or maintained by a covered entity whether in print, orally or electronically, and includes:

- "Individual identifiers" that clearly identify an individual (or has components that could be used to identify the individual, and
- Is related to a past, present, or future physical or mental health condition, or the provision of, or payment for health care or genetic information.

The following "individual identifiers," if used in any combination, create PHI:

Name	Geographic Indicators (smaller than a state)
Social Security Number (SSN)	Certificate/License Numbers
Date of Birth	Vehicle Identifiers
Date of Hire	URLs
Dates of Service	IP Address Numbers
Telephone or Fax Numbers	Biometric Identifiers
E-mail Address	Photographic Image
Medical Record Number	Other unique identifying numbers of codes
Health Plan Beneficiary Number	

Please note the following additional information:

- CSU's sponsored health benefit plans (medical, dental, and vision) have been subject to the HIPAA privacy regulations since April 14, 2003. The Health Care Reimbursement Account (HCRA) plan and campus-sponsored external Employee Assistance Programs (EAPs) became subject to the regulations on April 14, 2004.
- HIPAA does not apply to 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, accommodations for disabilities, FMLA or other leaves, workers' compensation, short and/or long term disability claims, life insurance, disability

pensions, and 401 (b) medical hardship withdrawals) and is used for normal human resources purposes. However, this information must still be protected.

- The privacy regulations do affect the scope of information that the health benefit plan providers (i.e., CalPERS medical, Delta Dental PPO, DeltaCare USA, Vision Service Plan (VSP) 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. To limit the campus' exposure of PHI information related to HCRA claims, campuses should instruct employees to file appeals directly with ASI, the third party administrator.
- 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.
- At the CSU, HIPAA privacy regulations are enforced by the CSU HIPAA Privacy Official within Human Resources Management (HRM) in the Chancellor's Office. At the campus level, the HIPAA Privacy Contact for human resources and benefits is primarily the Benefits Officer.
- Systemwide training will be held on an annual basis, and is mandatory for individuals that have access to PHI as a part of their job duties. A list of attendees will be maintained by the CSU HIPAA Privacy Official.

Physical and Technical Safeguards for Protecting PHI

When using or disclosing PHI, designated individuals should exercise extreme caution when handling PHI and make reasonable efforts to limit the amount of PHI deemed necessary for the intended purpose of its use and should use de-identified information whenever possible.

Below are some best practices to follow in protecting PHI:

- PHI should be discarded in such a manner that it cannot be retrieved (i.e., cross-cut shredded, locked disposal bins, etc.);
- For physical PHI (i.e., hard copy paper documents, CDs, diskettes, tapes, notes, etc.,) copies should be limited and these items should be kept in locked drawers/cabinets when away from the workstation, and discarded through appropriate means when no longer needed;
- If documents must be kept for extended periods, then they should be stored in an area with limited access;
- PHI should be discarded in such a manner that it cannot be retrieved (i.e., cross-cut shredded, locked disposal bins, etc.);
- If utilizing a facsimile (fax) machine, it should be located in an area with limited access and designated for a specific function (i.e., fax machine located in human resources or benefits office).

- Limit verbal discussions of PHI unless absolutely necessary, and restrict the usage of speakerphone to convey PHI to another party if working in a cubicle environment. Use discretion when leaving voicemail messages that contain elements of PHI.

Individual Rights and HIPPA Forms

The HIPAA Privacy Rule provides individuals (employees) with certain rights associated with their PHI that the CSU must follow. These include the rights to:

- Access, inspect, and copy certain PHI within a Designated Record Set;
- Request the Amendment of their PHI in a Designated Record Set;
- Request restriction of the use and disclosure of their PHI;
- Request the use of alternative means or alternative locations for receiving communications of their PHI; and,
- Request an accounting of PHI disclosures.

Information and associated forms regarding Individual Rights under HIPAA Privacy regulations can be located in sections 6 and 11 of the HIPAA Privacy Manual.

HIPAA Security Regulations – Impact on the CSU

The HIPAA Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting (electronic) e-PHI.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by employees.

The HIPAA Security Rule defines “confidentiality” to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, “integrity” means that e-PHI is not altered or destroyed in an unauthorized manner. “Availability” means that e-PHI is accessible and usable on demand by an authorized person only.

Physical and technical safeguards for e-PHI include the implementation of policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information. Some examples of these safeguards are as follows:

- Limitation of physical access to facilities to ensure that only authorized access is allowed;
- Proper use of and access to Workstation and Device security;
- Requirement of unique User IDs and passwords in order to access and/or transmit e-PHI. Employees are prohibited from sharing User IDs and/or passwords. In addition, access to such information must be terminated when the employee either: 1) no longer is assigned to a role within CSU that requires such access; or 2) ends employment with CSU;

- Encryption (i.e., PGP Desktop software) of e-PHI is required, and must be "destroyed" in such a manner that the information cannot be retrieved (i.e., PGP Desktop "shred file" feature);
- Technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network;
- Use of "Locking screensavers" to limit access to desktop and/or laptop computers when away from the workstation;
- Limit use of PHI in e-mails as much as possible.
- Audit and Integrity controls, such as hardware, software and/or other mechanisms that record and examine access and other activities in information systems that contain or use e-PHI.

At the CSU, the HIPAA Security Rule is enforced by the Chief Information Security Officer at the Chancellor's Office, who also serves a dual role as the CSU HIPAA Security Official.

For additional information regarding the CSU's Information Security Policy, please refer to the following website: http://www.calstate.edu/icsuam/sections/8000/8050.0.shtml.

Breach Notification Rules and Obligations

The HITECH Act definition of a PHI breach is as follows:

> ***(A) IN GENERAL. The term "breach" means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.***

A breach of physical and/or ePHI can occur in the course of day to day operations and may be attributable to:

- Theft;
- Loss;
- Improper Disposal;
- Unauthorized Access/Disclosure; or
- Hacking/IT Incident; or
- Unknown or Other Reason(s).

If a breach of physical PHI or ePHI occurs, it must be reported immediately upon discovery to the CSU HIPAA Privacy and HIPAA Security Officials at the Chancellor's Office, and campus Information Security Officer (ISO). The campus HIPAA Privacy Contact must also forward a completed Breach Incident Report Form to the CSU HIPAA Privacy and Security Officials at the Chancellor's Office (see sections 7.05 and 11.07 of the HIPAA Privacy Manual), and record the incident in the Breach log, located in the HIPAA Manual.

Typically, breaches that impact fewer than 500 individuals are reported on an annual basis to HHS, and must be reported to the impacted individuals within 60 days of discovery. Breaches that impact 500 or more individuals must be reported to HHS, the media and the impacted individuals within 60 days of discovery. The CSU Privacy Official and CSU Security Official will evaluate the breach to determine if breach notice rules are applicable, and will provide campus guidance accordingly, with regard to reporting to appropriate agencies, and the development of required breach notice(s) for impacted individuals.

Please note that not all HIPAA-related privacy and security incidents solicit an initiation of breach notification requirements under the HITECH Act.

CSU HIPAA Privacy Official

Name:	**Michelle Hamilton**
Title:	**Manager, Benefits and HR Programs**
Address:	**CSU Office of the Chancellor** **Human Resources Management** **401 Golden Shore** **Long Beach, CA 90802**
Phone:	**562/951-4413 or 562/951-4411**
Facsimile:	**562/951-4954**
E-mail:	**mhamilton@calstate.edu**

CSU HIPAA Security Official

Name:	**Cheryl Washington**
Title:	**CSU Chief Information Security Officer**
Address:	**CSU Office of the Chancellor** **401 Golden Shore** **Long Beach, CA 90802**
Phone:	**562-951-4190**
Facsimile:	**562-477-5951**
E-mail:	**cwashington@calstate.edu**

Campus HIPAA Privacy Contacts

Each campus, including the Chancellor's Office has a HIPAA Privacy Contact. The campus HIPAA Privacy Contact for human resources and benefits is the campus Benefits Officer.

Campus HIPAA Security Contacts

Each campus, including the Chancellor's Office has a designated Information Security Officer (ISO). Please contact either the Information Security Office at the respective campus or the Chief Information Security Officer at Chancellor's Office.

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 is currently available online for viewing at:
http://www.calstate.edu/Benefits/carrier.materials/HIPAAPrivacyManual_Campus.pdf.

Revised CSU 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, as amended by the HITECH Act.

HIPAA Privacy and Security Training: A PowerPoint presentation of the March 9, 2010, training webcast is available at: (URL to be determined). The recorded version of this webcast is also available on Systemwide Professional Development's website at: http://centralstationu.calstate.edu/howthingswork/ (User ID and password is required).

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 is available at: http://www.calstate.edu/HRAdm/pdf2011/HR2011-07AttE.pdf.

The HIPAA Privacy Manual should be read carefully and in-depth by CSU employees that have access to PHI as part of assigned duties.

Additional Resources

Full Text of HIPAA Regulations:

- The HIPAA Privacy Rule is located at 45 CFR Part 160 and Part 164, and can be downloaded at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt.
- The HIPAA Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164, and can be downloaded at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.
- The combined HIPAA Privacy and Security Regulations can be downloaded at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

Full Text of HITECH Act:

- The full text of the HITECH Act can be downloaded at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

Data Security Practices:

- **"Top Ten Good Security Practices:"** The Chancellor's Office Information Security Management developed a list of pertinent information on security practices when handling and/or accessing sensitive information, which can be downloaded at http://www.calstate.edu/HRAdm/pdf2011/HR2011-07AttH.pdf.