


Date: June 22, 2011

Code: HR 2011-07

Supersedes: HR-2004-22

To: CSU Presidents

From: Gail E. Brooks 
Vice Chancellor
Human Resources

Subject: HIPAA Regulations as Amended by the HITECH Act – Update of Privacy and Security Compliance for CSU Human Resources Operations

Overview

Audience: Human Resources Officers, Benefits Officers, and/or campus designee(s) responsible for human resources operations, including benefits administration.

Action Items: Campuses are required to adhere to HIPAA, as amended by HITECH, regarding privacy and security compliance obligations.

Affected Employee Groups/Units: All employees

Summary

The California State University is mandated by federal law to comply with the federal Standards for Privacy of Individually Identifiable Health Information (PHI) under Title II of the Health Insurance Portability and Accountability Act of 1996 (known as HIPAA), as amended by the HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009). The HITECH Act augments HIPAA's privacy and security related components; establishes breach reporting requirements; applies HIPAA privacy and security requirements and penalties to business associates; and is an expansion of HIPAA rules and obligations. Therefore, this document should be read in its entirety.

This letter updates privacy and security compliance obligations related to the California State University's (CSU) human resources operations, established under the Health Insurance Portability and Accountability Act (HIPAA), 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.

The HITECH Act:

- 1) Applies the same HIPAA privacy and security requirements (and penalties) for covered entities to business associates, and mandates that 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;

Distribution:

Chancellor Reed
All Campus Vice Presidents
AVPs/Deans, Faculty Affairs

Human Resources Officers
Payroll Managers
Campus Information Security Officers (ISO)

Campus Benefits Officers

- 3) Establishes mandatory federal privacy and security breach reporting requirements for entities subject to HIPAA compliance, including business associates;
- 4) Requires security breaches be reported to the media, if the number of impacted individuals is 500 or more;
- 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. See the fine structure below:

Type of Violation	Each Violation	All such violations of an identical provision in a calendar year
Due to Unknowing Violation	\$100 - \$50,000	\$1,500,000
Due to reasonable cause but not willful neglect	\$1,000 - \$50,000	\$1,500,000
Due to willful neglect that is timely corrected	\$10,000 - \$50,000	\$1,500,000
Due to willful neglect if not timely corrected	\$50,000	\$1,500,000

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. At the CSU, the HIPAA Privacy Rule is enforced by the CSU HIPAA Privacy Official within Human Resources Management (HRM), in the Chancellor's Office. Additional information regarding HIPAA Privacy regulations and safeguarding PHI can be located in the CSU HIPAA Policy (Attachment A), and the HIPAA Privacy Manual (Attachment B).

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.

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>, and the CSU HIPAA Policy.

CSU Privacy Notice

In accordance with HIPAA guidelines, the CSU revised its Privacy Notice (see Attachment C) and released an electronic copy to campuses on February 26, 2010, with instructions to provide a copy to all new hires. Human Resources Management (HRM) coordinated a mass mailing of the revised Notice to all current employees that was completed in early March 2010.

Business Associate Agreement

In a previous HR Letter (HR 2004-22), it was established that HIPAA privacy compliance extended to the Health Care Reimbursement Account (HCRA) plan and external campus-sponsored Employee Assistance Programs (EAP), in addition to business associates. As a result of the HITECH Act, these entities are now subject to the same HIPAA privacy and security requirements (and penalties) that were previously limited to covered entities, and it mandates that security obligations be incorporated into all business associate contracts.

Consequently, CSU released two electronic versions of the revised CSU Business Associate Agreement (see Attachment D) to campuses on February 26, 2010, which included required HITECH language. Campuses were instructed to obtain a signed copy of either the Business Associate Agreement or the Business Associate Agreement Amendment (as deemed appropriate) and forward a copy to Human Resources Management in the Chancellor's Office. In the future, if the campus replaces its current EAP provider, or establishes an EAP program and secures an external EAP provider, a signed copy of the business associate agreement must be forwarded to the CSU HIPAA Privacy Official.

The following campuses utilize an external EAP: CSU Bakersfield; CSU Channel Islands; CSU Dominguez Hills; CSU East Bay; CSU Humboldt; CSU Los Angeles; CSU Maritime Academy; San Diego State University; San Jose State University; San Luis Obispo; CSU San Marcos; Sonoma State University; and CSU Stanislaus.

The CSU HIPAA Privacy Official also maintains a signed copy of the Business associate Agreement for the third party administrator of the HCRA plan.

Breach Notification Requirements

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.

If a breach of physical PHI or ePHI occurs, it must be reported immediately upon discovery to the CSU HIPAA Privacy and CSU HIPAA Security Officials at the Chancellor's Office, and the 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 CSU HIPAA 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, also 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 HIPAA Privacy and CSU HIPAA Security Officials 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.

HIPAA Privacy and Security Training Webcast

To prepare campuses for the changes made by HITECH to HIPAA Privacy and Security rules, HRM, in collaboration with its benefits consultant Mercer, held a HIPAA Privacy and Security Training Webcast on March 9, 2010. The training provided an overview of the privacy and security rules, best practices for safeguarding PHI, in addition to information regarding the breach notification rules. This webcast was recorded and access is available (with User ID and Password) at: <http://centralstationu.calstate.edu/>. Campus individuals that need access to this training module should contact the CSU HIPAA Privacy Official to obtain a User ID and password.

CSU HIPAA Privacy and Security Policy Components

The CSU HIPAA and Security Policy are comprised of several pertinent documents provided as Attachments listed below:

Attachment A: Revised CSU HIPAA Privacy Policy

The revised CSU HIPAA Privacy Policy has been updated with pertinent information regarding the HITECH Act, safeguards for protecting physical and electronic PHI, identifies the CSU HIPAA Privacy Official and CSU HIPAA Security Official, and provides breach notification instructions.

Attachment B: HIPAA Privacy Manual

The revised CSU HIPAA Privacy Manual has been updated with HITECH Act information and references; and contact information of the CSU HIPAA Privacy Official. This version also contains additional HIPAA forms, including breach notification and breach log. Though it is comprehensive, it should be read in its entirety.

Attachment C: Revised HIPAA Privacy Notice

The revised HIPAA Privacy Notice, as previously stated, has been updated with appropriate HITECH language. Campuses should continue distributing this version to new hires, or to any employee that requests a copy.

Attachment D: Revised Business Associate Agreements

The revised HIPAA Privacy and Business Associate Agreement and the HIPAA Business Associate Agreement Amendment contain updated HITECH language regarding HIPAA privacy and security.

Attachment E: Revised "Authorization to Use and/or Disclose Personal Health Plan Information" Form

The revised "*Authorization to Use and/or Disclose Personal Health Plan Information*" form has been updated with the appropriate CSU logo. A signed authorization must be obtained from an employee if the Benefits office is assisting an employee with a health care related claim, or if PHI must be used for purposes deemed necessary by HIPAA Privacy rules.

Attachment F: HIPAA Privacy and Security Training Presentation

The PDF version of the HIPAA Privacy and Security Training Webcast PowerPoint presentation provides an overview of HIPAA Privacy and Security, and a copy should be provided to new human resources and/or benefits staff.

Attachment G: 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 (see attached list).

Attachment H: Data Security Practices

The Chancellor's Office Information Security Management developed a list of "**Top Ten Good Security Practices**," with pertinent information on security practices when handling and/or accessing sensitive information.

CSU HIPAA Privacy Official and CSU HIPAA Security Official

The designated CSU HIPAA Privacy Official and CSU HIPAA Security Official are as follows:

CSU HIPAA Privacy Official:	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:	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

The contact information for each campus' Information Security Officer can be obtained by either contacting the Information Security Office at the respective campus, or the CSU Chief Information Security Officer located at the Chancellor's Office.

Additional Resources

- 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/privacylet.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/privacylet/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>.

Additional Information

DCRA/HCRA Administrative Guide has been updated to reflect the HIPAA and HITECH regulations, and will be issued to campuses in a separate communication.

As mentioned, campus human resources departments are encouraged to review the HIPAA Privacy manual, HIPAA Privacy and Security Policy and other HIPAA-related materials outlined in this HR Letter to ensure compliance with the regulations. If you have questions, please call the CSU HIPAA Privacy Official at (562) 951-4413.

Please note: HIPAA Privacy and Security information with impact to additional departments within CSU is forthcoming.

This memorandum and attachments are also available on the Human Resources Management's Web site at:
<http://www.calstate.edu/HRAdm/memos.shtml>.

GEB/mh

Attachments

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	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – Applies if they transmit health data electronically – Can include on-site clinics and medical facilities – Includes applicable CSU Student Health Centers
Health Care Clearinghouses	<ul style="list-style-type: none"> – 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
<p>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.</p> <p>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.</p>

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 HIPAA 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

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/privrule.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/adminsimplereqtext.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>.

California State University

HIPAA Privacy Manual

Revised February 17, 2010

As prepared by

MERCER



MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

The HIPAA Privacy Manual was drafted for the exclusive use of California State University (CSU) to assist CSU in complying with the federal Standards for Privacy of Individually Identifiable Health Information under Title II of the Health Insurance Portability and Accountability Act of 1996 (known as HIPAA), as amended by the HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009).

Any reproduction or other use for commercial or other purposes is not permitted without the express written permission of Mercer Health & Benefits LLC (Mercer).

Table of Contents

1. Introduction	1
2. Definitions.....	3
2.01 Definitions	4
3. Statement of Privacy Policy	9
4. Safeguards.....	10
4.01 Overview	11
4.02 Protection Procedures	12
4.03 Verification Procedures	14
a. Citations	15
5. Uses and Disclosures	16
5.01 Overview	17
a. Citations	18
5.02 Enrollment, Premium Bids, Amendment/Termination Activities.....	19
a. Citations	20
5.03 Treatment, Payment, and Health Care Operations	21
a. Appeals of Adverse Benefit Determinations	22
b. Customer Service	23
c. Data Analysis	24
d. Citations	24
5.04 When Authorizations are Needed	26
a. Citations	26
5.05 Disclosure to Participants, Beneficiaries, and Others Acting on Their Behalf	27
a. Participants	27
b. Personal Representatives	27
c. Others Acting on a Participant's Behalf.....	28
d. Citations	28
5.06 List of Legally Required Uses, Public Health Activities, Other Situations Not Requiring Authorization ..	29
5.07 Use and Disclosure of De-Identified Information and Data Use Agreements.....	32
a. De-Identified Information.....	32
b. Data Use Agreements	33
c. Citations.....	34
5.08 Reporting Improper Access, Uses and Disclosures.....	35
a. How to Report a PHI Breach.....	35
b. What Information to Include in a Breach Report.....	35
c. When to Submit a Breach Report	35
d. Documentation.....	35
e. Citations.....	35
6. Individual Rights.....	37
6.01 Overview	38
6.02 Inspect and Copy PHI.....	39
a. Participant's Right.....	39
b. Processing a Request.....	39
c. Accepting a Request to Access, Inspect, or Copy	40
d. Denying a Request to Access, Inspect, or Copy (Where Participant has Right to Review)	40
e. Denying a Request to Access, Inspect, or Copy (Where Participant has NO Right to Review).....	41
f. Form for Denial	42
g. Documenting Requests	42
h. Citations	42

6.03 Amend PHI	43
a. Participant's Rights	43
b. Processing a Request	43
c. Amending PHI and Notifying Others	43
d. Denying an Amendment	44
e. Documenting Requests	44
f. Citations	45
6.04 Restricted Use of PHI	46
a. Participant's Rights	46
b. Receiving a Request	46
c. Processing a Request	46
d. Documenting Requests	46
e. Citations	47
6.05 Confidential Communications	48
a. Participant's Rights	48
b. Processing a Request	48
c. Documenting Requests	48
d. Citations	49
6.06 Accounting of Non-Routine Disclosures	50
a. Participant's Rights	50
b. Processing a Request	50
c. Content of the Accounting	51
d. Documenting Requests	52
e. Citations	52
7. Risk Management Activities	53
7.01 Overview	54
7.02 Training	55
a. When Training will Occur	55
b. Contents of Training	55
c. Documentation	56
d. Citations	57
7.03 Complaints	58
a. Filing Complaints	58
b. Processing Complaints and Complaint Resolution	58
c. Documentation	59
d. Citations	59
7.04 Sanctions	60
a. Determining Sanctions	60
b. Documentation	60
c. Citations	60
7.05 Mitigation of PHI Breaches	61
a. Investigating Reported Breaches Originating from CSU	61
b. Assessing Whether the Incident Requires CSU to Send Breach Notices	61
c. Preparing Breach Notices	63
d. Distributing Breach Notices	64
e. Reporting Breach Incidents to HHS	65
f. Mitigation Steps for Breaches Originating from a Business Associate	65
g. Documentation	65
h. Citations	65
7.06 Document Retention	66
a. Document Retention Checklists	66
b. Citations	68

8. Required Legal Documents	69
8.01 Overview	70
8.02 Privacy Notice	71
<i>a. Identifying the Recipients</i>	<i>71</i>
<i>b. Distributing the Notice.....</i>	<i>71</i>
<i>c. Revising the Notice.....</i>	<i>71</i>
<i>d. Informing Participants of the Availability of the Notice</i>	<i>72</i>
<i>e. Documenting Notices.....</i>	<i>72</i>
<i>f. Citations</i>	<i>72</i>
8.03 Authorization.....	73
<i>a. Providing the Authorization Form to Participants</i>	<i>73</i>
<i>b. Signing of the Authorization Form.....</i>	<i>73</i>
<i>c. Receiving the Signed Authorization Form.....</i>	<i>73</i>
<i>d. Determining the Validity of Authorization.....</i>	<i>73</i>
<i>e. Revocation of Authorization</i>	<i>74</i>
<i>f. Documentation Requirement.....</i>	<i>74</i>
<i>g. Citations</i>	<i>74</i>
9. Guidelines for Policy and Procedure Changes	75
10. HIPAA Resources	79
11. Key Resources and Forms	80
11.01 Covered Plans	81
11.02 Privacy Official	81
<i>a. Privacy Official Designation.....</i>	<i>81</i>
<i>b. Sample Privacy Official Job Description</i>	<i>82</i>
<i>c. Essential Duties - General.....</i>	<i>82</i>
<i>d. Essential Duties – Specific.....</i>	<i>82</i>
11.03 Other Contacts.....	84
11.04 Insurers	85
11.05 Notice of Privacy Practices.....	86
11.06 Participant Forms	93
<i>a. Request for Access to Inspect and Copy.....</i>	<i>94</i>
<i>b. Request to Amend Personal Health Plan Information.....</i>	<i>97</i>
<i>c. Restricted Access.....</i>	<i>100</i>
<i>d. Request for Confidential Communications.....</i>	<i>103</i>
<i>e. Accounting of Non-Routine Disclosures</i>	<i>106</i>
<i>f. Authorization for Use and/or Disclosure of Health Information</i>	<i>109</i>
11.07 Breach Report Forms.....	113
<i>a. Breach Incident Report Form</i>	<i>114</i>
<i>b. Breach Incident Log</i>	<i>117</i>

1. Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009), required the US Department of Health and Human Services (HHS) to establish rules to protect the privacy of health information. HHS issued detailed rules (referred to throughout this Manual as the HIPAA Privacy Rule), for health plans, health care providers, and certain other health care entities (known as Covered Entities). Health information covered by the HIPAA Privacy Rule is known as Protected Health Information (PHI).

Words and phrases that are capitalized in this Manual, such as “Covered Entities,” have special meanings that are defined in Section 2.

California State University (CSU) sponsors the group health plan(s) listed in Section 11.01 and each plan is a Covered Entity. Health plans and other Covered Entities are required to create Policies and Procedures to ensure their compliance with the HIPAA Privacy Rule. This Manual is designed to be the Policies and Procedures for the health plan(s) in Section 11.01, referred to throughout as the “Plan”. Because each plan is sponsored by CSU, they collectively comprise an “organized health care arrangement” and the Manual represents the Policies and Procedures for each plan. The HIPAA Privacy Rule and this Manual are effective on and after April 14, 2003, for all the group health plans sponsored by CSU except for the external Employee Assistance Plans (EAPs) and the Health Care Reimbursement Account Plan (HCRA). The effective date for the external EAP and HCRA plans is April 14, 2004. This Manual is updated as of February 17, 2010.

CSU’s health benefit plans insurers and HMOs are Covered Entities under the HIPAA Privacy Rule and as such must establish privacy policies and procedures. However, the HCRA plan is self-insured. Therefore, CSU (as the HCRA plan sponsor) is primarily responsible for the HCRA plan’s compliance with the HIPAA Privacy Rule. Although the external EAPs are not considered insured plans for HIPAA Privacy purposes, CSU has very limited HIPAA Privacy obligations for the external EAPs. CSU does not receive any Protected Health Information from the external EAPs.

The Manual consists of twelve (11) sections.

Section 1, this introduction, describes the purpose of the Manual and its organization.

Section 2 defines key terms that are used in this Manual. The defined terms are capitalized throughout the Manual. *In general, the term Participant is used to refer to persons who are or were eligible for benefits under the Plan. Participant is used to refer to both employee Participants and other beneficiaries, unless the context clearly indicates otherwise.*

Section 3 describes the Plan's overall policy for protecting the use and disclosure of health information.

Sections 4 and 5 describe the basic requirements that apply to the Plan's use and disclosure of PHI. The sections also describe the procedures CSU will use when handling health information for the Plan.

Section 6 describes certain rights that Plan Participants and their beneficiaries have concerning their own PHI, and the Plan's procedures for administering those rights.

Sections 7 and 8 describe risk management requirements that the Plan must meet and documentation that the Plan must maintain. The sections also describe CSU's risk management activities for actions it performs on the Plan's behalf.

Section 9 contains links to the text of regulations related to implementation of this Manual.

Section 10 contains the text of the HIPAA Privacy Rule.

Section 11 contains key resources related to the implementation of this Manual. It includes the name of the Privacy Official responsible for the development, coordination, implementation, and management of the Manual. It also includes key contacts (the Campus Privacy Contacts) responsible for receiving requests from Participants exercising their rights described in Section 6, for receiving complaints about the Plan's compliance with the Manual or with the HIPAA Privacy Rule, and for processing any specific Authorizations that Participants may be asked to provide concerning the use of their PHI. Finally, it includes the forms and other Plan Documents that CSU will be using to meet the privacy requirements, along with instructions for using those forms.

The Manual or a summary thereof will be provided to employees of CSU who have access to PHI. Employees can obtain more information from the Plan's Privacy Official and other contacts listed in Section 11.

*Health information collected by CSU pursuant to other laws such as the Family and Medical Leave Act, Americans with Disabilities Act, Occupational Safety and Health Act, or workers' compensation laws, is **not** protected under HIPAA as PHI (although this type of information may be protected under other federal or state laws). Employees should consult the appropriate Campus Privacy Contact for privacy policies governing employee information not connected with the Plan.*

2. Definitions

2.01 Definitions

Authorization: A person's permission to use PHI for purposes *other* than Treatment, Payment, or Health Care Operations, or as otherwise permitted or required by the HIPAA Privacy Rule (see Section 5). Authorizations require specific contents described in Section 8.06.

Amendment: A change or modification.

Breach Notice Rule: Regulations that mandate notice to individuals in some cases if their PHI is improperly accessed, used, or disclosed, as well as a report to HHS of such incidents. Media notice may also be required. The notice/report contents, timing, and distribution requirements are prescribed by the Breach Notice Rule.

Business Associate: A person or entity that performs a function or activity regulated by HIPAA on behalf of the Plan and involving individually identifiable health information. Examples of such functions or activities are claims processing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services. A person or entity that transmits PHI to a Covered Entity (or its Business Associate) and routinely requiring access to that PHI may also be a Business Associate. Examples of such entities include health information exchange organizations, regional health information organizations and e-prescribing gateways. Vendors that contract with Covered Entities offering certain personal health records to individuals may also be considered Business Associates. A Business Associate may be a Covered Entity. However, Insurers and HMOs are not Business Associates of the plans they insure. The HIPAA Privacy Rule requires that each Business Associate of the Plan enter into a written contract (Business Associate Agreement) with the Plan before the Plan can disclose PHI to it, as described in Section 8.05.

Campus Privacy Contact: The persons or offices described in Section 11.03 who are responsible for responding to Participants exercising their rights described in Section 6 and for other duties specified in Section 11.03.

Confidential Communication: An alternative means or alternative locations to communicate PHI to the Participant. See Section 6.05 for more information.

Covered Entity: A health plan (including an employer plan, Insurer, HMO, and government coverage such as Medicare); a health care provider (such as a doctor, hospital, or pharmacy) that electronically transmits any health information in connection with a transaction for which HHS has established an EDI (electronic data interchange) standard; and a health care clearinghouse (an entity that translates electronic information between nonstandard and HIPAA standard transactions).

De-identification: The removal of personal information (such as name, Social Security number, address) that could identify an individual. The HIPAA Privacy Rule lists eighteen

(18) identifiers that must generally be stripped for data to meet the De-identification safe harbor described in Section 5.07.

Designated Record Set: A group of records that the Plan (or its Business Associate) maintains that relates to enrollment, Payment, claims adjudication, and case or medical management records, or that the Plan (or its Business Associate) uses, in whole or in part, to make decisions about Participants. The Plan has identified specific Designated Record Sets for particular uses (see Section 6.02).

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI outside of the Plan.

Electronic Health Record. An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

ERISA: The Employee Retirement Income Security Act of 1974, as amended.

Fiduciary: A person or entity that exercises any discretionary authority or discretionary control respecting management of the Plan or disposition of its assets; renders investment advice for a fee or other compensation, direct or indirect, with respect to any moneys or other property of the Plan, or has authority or responsibility to do so; or has discretionary authority or discretionary responsibility in the administration of the Plan. A Fiduciary can be an individual, partnership, joint venture, corporation, mutual company, joint-stock company, trust, estate, association, unincorporated organization, or employee organization. A person can be deemed a Fiduciary by performing the acts described above with or without authority to do so, by holding certain positions with duties and responsibilities similar to the acts described above, or by being expressly designated or named as a Fiduciary in the Plan Document.

Health Care Operations: Activities related to a Covered Entity's functions as a health plan, health provider, or health care clearinghouse. They include quality assessment and improvement activities, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, business planning and development (such as cost management), customer service, grievance and appeals resolution, vendor evaluations, legal services.

HHS: The United States Department of Health and Human Services.

HIPAA Privacy Rule: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes "administrative simplification" rules that will affect the way group health plans and their vendors use, disclose, transmit, and secure health information. The administrative simplification rules include: privacy protections; rules governing transmission of electronic health care data (electronic data interchange or "EDI" rules); and rules that apply new security standards to health information. The "HIPAA Privacy Rule" refers to the new privacy protections of HIPAA.

Insurer: An underwriter, insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a state and is subject to state law that regulates insurance. This term does not include a group health plan.

Limited Data Set. A limited data set is PHI that **excludes** all of the following direct identifiers: Names; postal address information, except town or city, state, and zip code; telephone numbers; fax numbers; e-mail addresses; Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Web URLs; IP addresses; biometric identifiers, including finger and voice prints; and full-face photographic images and any comparable images.

Marketing: An arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI for the other entity or its affiliate, in exchange for direct or indirect remuneration, to make a communication about its own product or service that encourages purchase or use of that product or service. Marketing is also a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, except for communication made:

- To describe a health-related product or service (or payment for such product or service) that is provided by, or included in the benefits of, the Plan, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, the Plan; and health-related products or services available only to a Plan enrollee that add value to, but are not part of, the Plan's benefits;
- For Treatment; or
- For case management or care coordination for the person, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the person.

However, the exceptions described above will not be excluded from the definition of Marketing if the Covered Entity receives or has received direct or indirect payment in exchange for making such communication, except where (i) such communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment received by such Covered Entity in exchange for making a communication is a reasonable amount; (ii) the communication is made by the Covered Entity and the Covered Entity obtains from the recipient of the communication a valid Authorization for that communication; or (iii) the communication is made by a Business Associate on behalf of the Covered Entity and the communication is consistent the written Business Associate Agreement between the Covered Entity and the Business Associate.

Minimum Necessary: To the extent practical, Covered Entities are expected to make a reasonable effort to limit uses and disclosures of, and requests for, PHI to the minimum amount of information needed to support the purpose of the use, disclosure, or request. Effective February 17, 2010, the Minimum Necessary amount of PHI used, disclosed or requested by the Plan will be restricted to a Limited Data Set, to the extent practical to accomplish the intended purpose of the transaction. If more than a Limited Data Set is needed, workforce members will exercise their judgment about the amount of PHI needed to accomplish the intended purpose of the transaction and restrict the PHI used, disclosed, or requested to such greater amount and that greater amount will be treated as the Minimum Necessary for that transaction.

Participant: Persons who are or were eligible for benefits under the Plan. Participant refers to both active employees who are members of the Plan and other beneficiaries, unless the context clearly indicates otherwise.

Payment: Activities by a plan to obtain premiums or determine or fulfill its responsibility for coverage and the provision of benefits under the Plan. Also, activities by a plan or provider to obtain or provide reimbursement for the provision of health care. These activities include determinations of eligibility or coverage, adjudication or subrogation or health benefit claims, billing, claims management, collection activities, reinsurance payment, review of health care services with respect to medical necessity, review of coverage under a health plan, review appropriateness of care or justification of charges, and utilization review activities.

Plan: The health plan for which these Policies and Procedures were written.

Plan Document: A written document that sets forth a plan's terms and conditions.

Plan Sponsor: The employer, employee organization, or the association, committee, joint board of trustees, or other similar group of representatives, that established or maintain the Plan.

Policies and Procedures: Descriptions of the Plan's intentions and process for complying with the HIPAA Privacy Rule and Breach Notice Rule, as codified in this Manual.

Privacy Official: A designated individual responsible for the development and implementation of the Plan's privacy Policies and Procedures.

Privacy Notice: A description, provided to Participants at specific times, and to other persons upon a request of the Plan's practices concerning its uses and disclosures of PHI, which also informs Participants of their rights and of the Plan's legal duties, with respect to PHI.

Protected Health Information (PHI): Individually identifiable health information created or received by a Covered Entity. Information is "individually identifiable" if it names the

individual person or there is a reasonable basis to believe components of the information could be used to identify the individual. “Health information” means information, whether oral or recorded in any form or medium, that (i) is created by a health care provider, plan, employer, life insurer, public health authority, health care clearinghouse, or school or university; and (ii) relates to the past, present, or future physical or mental health or condition of a person, the provision of health care to a person; or the past, present, or future Payment for health care.

Psychotherapy Notes: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record. It excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Treatment: The provision, coordination, or management of health care by one (1) or more health care providers. It includes health care coordination or management between a provider and a third party, as well as consultation and referrals between providers.

3. Statement of Privacy Policy

The Plan will protect the privacy of Participant and family member health information (known as Protected Health Information or PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). PHI generally will be used only for health plan Payment activities and operations, and in other limited circumstances such as where required for law enforcement and public health activities. In addition, the Minimum Necessary information will be used except in limited situations specified by law. Other uses and disclosures of PHI will not occur unless the Participant authorizes them. Participants will have the opportunity to inspect, copy, and amend their PHI as required by HIPAA. Participants can exercise the rights granted to them under HIPAA free from any intimidating or retaliatory acts.

When PHI is shared with Business Associates providing services to the Plan, they will be required to agree in writing to maintain procedures that protect the PHI from improper uses and disclosures in conformance with HIPAA.

When CSU receives PHI to assist in Plan administration, it will adhere to its own stringent procedures to protect the information. Among the Procedures in place are:

- Administrative and technical firewalls that limit which groups of employees are entitled to access PHI and the purposes for which they can use it;
- Rules for safeguarding PHI from improper disclosures;
- Processes to limit the disclosure of PHI to the Minimum Necessary;
- A verification process to identify and confirm the authority of persons requesting PHI;
- A training process for relevant staff; and
- Processes for filing privacy complaints.

The Plan may update this Policy and its Procedures at any time. The Plan will also update this Policy and its Procedures to reflect any change required by law. Any changes to this Policy and Procedures will be effective for all PHI that the Plan may maintain. This includes PHI that was previously created or received, not just PHI created or received after the Policy and Procedures are changed.

4. Safeguards

4.01 Overview

4.02 Protection Procedures

4.03 Verification Procedures

4.01 Overview

The Plan will develop and implement administrative, technical, and physical safeguards that will reasonably protect Protected Health Information (PHI) from intentional and unintentional uses or disclosures that violate the HIPAA Privacy Rule. In addition, the Plan will institute procedures to verify the identity of any person or entity requesting PHI and the authority of that person or entity to have access to PHI.

PHI is individually identifiable health information created or received by a Covered Entity. Information is “individually identifiable” if it identifies the individual or there is a reasonable basis to believe components of the information could be used to identify the individual. “Health information” means information, whether oral or recorded in any form or medium, that (i) is created or received by a health care provider, health plan, employer, life insurer, public health authority, health care clearinghouse or school or university; and (ii) relates to the past, present, or future physical or mental health or condition of a person, the provision of health care to a person, or the past, present, or future Payment for health care.

Sections 4.02 and 4.03 describe the Procedures CSU will use to establish safeguards and to verify identification and authority when using PHI. Insurers and Business Associates of the Plan will also adopt procedures that meet the requirements of the HIPAA Privacy Rule.

4.02 Protection Procedures

CSU will apply the following Procedures to protect PHI:

Protected information	Protection procedures
Printed/ hard copy documentation	<ul style="list-style-type: none"> • Funnel incoming mail with PHI to the correct department to limit access to PHI. • Limit the number of photocopies made of PHI. • Implement a “clean desk” practice. PHI will not be left in “plain site” on desks and computers (e.g., put away documents with PHI or turn them over when leaving your desk, exit computer files and e-mail with PHI before leaving your desk, etc.). Take measures to prevent unauthorized personnel from being able to view PHI on your desk and computer. • PHI that the Plan is required to retain for lengthy time frames will be kept in storage areas, with access limited to designated personnel. • PHI in paper format will be destroyed when it is obsolete or is not required to be retained for storage purposes, with shredding the preferred method of destruction.
E-mail and electronic storage (LAN/hard drive/diskettes)	<ul style="list-style-type: none"> • Destroy electronic PHI that is no longer needed, including cutting or destroying CDs or diskettes so that they are not readable. • Limit the use of PHI in e-mails, to the extent practical, to Limited Data Sets and exclude birth date and zip code data or, if needed, the Minimum Necessary to accomplish the intended purpose (e.g., refrain from forwarding strings of e-mail messages containing PHI. Instead, prepare a new message with only the amount of PHI described here). • Require password to get on the network. • Maintain and periodically update network monitoring software, including intrusion detection and reporting. • Maintain and periodically update systems for backing up data and contingency plans for data recovery in the event of a disaster. • Maintain and periodically update systems for tracking access and changes to data.

Protected information	Protection procedures
	<ul style="list-style-type: none"> Periodically review the process for handling system maintenance and the hardware/software acquisition process. Maintain and periodically update virus software and protection processes. Maintain and periodically review procedures for ending data access for staff (e.g., after they terminate employment). Follow other company IT guidelines regarding electronic data. Limit remote access to systems to secure methods
Facsimiles	<ul style="list-style-type: none"> Ensure that designated fax machines receiving PHI are not located in publicly accessible areas. Develop fax coversheet including confidentiality statement and warning about releasing data. Limit faxing of PHI to the Minimum Necessary. Notify the receiver in advance that CSU is sending a fax so he or she can retrieve it immediately. Check confirmation sheets to verify that outgoing faxes were received by the correct number.
Oral conversations/ telephone calls/voicemail	<ul style="list-style-type: none"> Limit the content of PHI in conversations (e.g., with vendors and other staff), as practical, to Limited Data Sets and exclude birth date and zip code data or, if needed, the Minimum Necessary to accomplish the intended purpose. Verify the identity of individuals on the phone (see Section 3.03). Implement reasonable measures to prevent other individuals from overhearing conversations. Limit voicemail messages, or messages with PHI left for other individuals to the amount Minimum Necessary.

4.03 Verification Procedures

In performing administration activities for the Plan, CSU will implement the following verification procedures to reasonably ensure the accurate identification and authority of any person or entity requesting PHI. Note that documentation of these verifications should be retained as provided in Section 7.06. Insurers and Business Associates will also institute verification procedures for disclosures of PHI. Refer to Section 5 for examples of PHI requests to the CSU.

Who makes the request	Procedure
Participants, Beneficiaries, and others acting on their behalf	CSU may obtain photo identification, a letter or oral Authorization, marriage certificate, birth certificate, enrollment information, identifying number, and/or claim number.
Health plans, providers, and other Covered Entities	CSU may obtain identifying information about the entity and the purpose of the request, including the identity of a person, place of business, address, phone number, and/or fax number known to the Plan.
Public officials *	For in-person requests, obtain agency identification, official credentials or identification, or other proof of government status. For written requests, verify they are on the appropriate government letterhead. Also obtain a written (or, if impracticable, oral) statement of the legal authority under which the information is requested. CSU will rely on the statements and documents of public officials unless such reliance is unreasonable in the context of the particular situation.
Person acting on behalf of a public official *	Obtain a written statement on appropriate government letterhead or other evidence or documentation of agency (such as a contract for services, memorandum of understanding, or purchase order) that establishes that the person is acting on behalf of the public official.
Person acting through legal process *	Obtain a copy of the applicable warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal.
Person needing information based on health or safety threats *	Consult with Privacy Official. Disclosure is permitted if, in the exercise of professional judgment, CSU concludes the disclosure is necessary to avert or lessen an imminent threat to health or safety, and that the person to whom the PHI is disclosed can avert or lessen that threat.

***Campus Privacy Contacts should notify the Privacy Official immediately if they receive any such request.**

a. Citations

45 CFR § 164.514(h)

§ 13405(b) of HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009)

5. Uses and Disclosures

5.01 Overview

5.02 Enrollment, Premium Bids, Amendment/Termination Activities

5.03 Treatment, Payment, and Health Care Operations

5.04 When Authorizations Are Needed

5.05 Disclosure to Participants, Beneficiaries, and Others Acting on Their Behalf

5.06 List of Legally Required Uses, Public Health Activities, Other Situations not Requiring Authorization

5.07 Use and Disclosure of De-Identified Information and Limited Data Sets

5.08 Reporting Improper Access, Uses, and Disclosures

5.01 Overview

This Section 5.01 summarizes limits imposed by the HIPAA Privacy Rule on the Plan's uses and disclosures of PHI. Sections 5.02 through 5.07 describe Procedures CSU maintains to satisfy the standards when it uses PHI on behalf of the Plan. Insurers and Business Associates will also adopt procedures to meet those standards, and Business Associates will act as described in their Business Associate Agreement (see Section 8.05). Section 5.08 provides a Procedure for alerting the Breach Contact to impermissible uses and disclosures.

In general, a Participant's PHI can be used or disclosed for a variety of Plan administrative activities. Common examples include resolving appeals and helping Participants address problems. The HIPAA Privacy Rule does not prohibit these activities, but it imposes the following guidelines:

Uses and disclosures generally allowed without Authorization. A person's PHI can be used or disclosed without obtaining that person's Authorization as follows:

- If disclosed to CSU for enrollment activities and (where only summary health information is used) for premium bids and Plan Amendment/termination activities;
- If requested by a Health Care Provider for Treatment;
- If needed for Payment activities such as claims, appeals and bill collection;
- If needed for Health Care Operations such as audits and wellness and risk assessment programs;
- If disclosed to the Participant, and in certain circumstances, to family members and others acting on the Participant's behalf; and
- If required by law, in connection with public health activities, or in similar situations as listed in Section 5.06. Campus Privacy Contacts will notify the Privacy Official immediately if they are required by law to disclose PHI.

Details on the types of activities that constitute permissible Treatment, Payment, and Health Care Operations are included in this Section 5 and in the Definitions. In some cases, the Plan will want to use or disclose PHI for other purposes, in which case Authorization will be required. In addition, except in certain limited circumstances, Authorization is required for the use and disclosure of Psychotherapy Notes and for the use and disclosure of PHI for Marketing.

Information is limited to the "Minimum Necessary." The Plan must limit uses and disclosures of PHI to the Minimum Necessary to accomplish the intended purpose. This

requirement does not apply to:

- Uses or disclosures for Treatment purposes;
- Disclosures to the Department of Health and Human Services (HHS) for audits of the Plan's compliance with the HIPAA Privacy Rule;
- Disclosures to an individual of his or her own PHI;
- Uses or disclosures required by law;
- Uses or disclosures made pursuant to an Authorization; and
- Uses or disclosures otherwise required for compliance with the HIPAA Privacy Rule.

De-identified Information. The limits in this Manual apply only to health information that is individually identifiable. If information is de-identified, it can then be used or disclosed without restriction. In addition, information that has most of its identifiers removed can be disclosed to a person signing a Data Use Agreement (see Section 5.07)

Improper Uses or Disclosures. The Plan's PHI cannot be properly used or disclosed except as described in this Manual. If CSU workforce members learn of a suspected or confirmed improper use or disclosure of PHI, they are required to take timely action so that CSU may meet its obligations to assess and address the incident (see Section 4.07).

a. Citations

45 CFR § 164.502(b)

45 CFR § 164.502(d)

45 CFR § 164.508

45 CFR § 164.514

45 CFR part 164, subpart D

§ 13405(b) of HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009)

5.02 Enrollment, Premium Bids, Amendment/Termination Activities

CSU will process Participant enrollment and disenrollment elections and transmit the elections to the Plan, its Insurers, and its Business Associates. The Plan, its Insurers and its Business Associates will, without obtaining a Participant's Authorization, disclose certain types of PHI (enrollment/disenrollment information and summary health information) to CSU (or its agents) in the following circumstances:

PHI disclosed	Employer uses of PHI
Enrollment and disenrollment information	<ul style="list-style-type: none"> Enrollment and disenrollment activities, including processing of annual enrollment elections, payroll processing of elected Participant contribution amounts, new-hire elections, enrollment changes, and responding to Participant questions related to eligibility for Plan enrollment.
Summary health information (see table below)	<ul style="list-style-type: none"> To obtain premium bids for health insurance coverage under the Plan (if CSU requests the information). To modify, amend, or terminate the Plan (if CSU requests the information).

The enrollment and disenrollment information and summary health information that CSU or its agents receives from the Plan will be subject to limits on further use or disclosure in accordance with CSU's general privacy policy, rather than the HIPAA Privacy Rule or the provisions of this Manual.

Required deletions for Summary Health Information		
Summary health information is information that summarizes claims history, expenses, or types of claims of individuals receiving benefits under the Plan from which the following information has been deleted.		
<ul style="list-style-type: none"> Names; Social Security numbers; Full face photographic and any comparable images; Telephone numbers; Specific dates such as dates of birth and death, and admission/discharge dates. <i>The Plan can use the year of the event, except for the birth year of persons over age eighty-nine (89)</i> 	<ul style="list-style-type: none"> Vehicle identifiers (serial number or license plate number); Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Fax numbers; E-mail address; Medical record number; Any other unique identifying numbers, or characteristics, or codes, including particular subsidiaries, divisions, or work locations 	<ul style="list-style-type: none"> Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Internet Protocol (IP) address numbers; Biometric identifiers (e.g., finger, iris, or voice prints); and Geographic identifiers smaller than a state, including street address, city, county, and precinct; but the five (5)-digit zip code may be used.

a. Citations

45 CFR § 164.504(f)(1)

5.03 Treatment, Payment, and Health Care Operations

The HIPAA Privacy Rule permits CSU to receive PHI (other than enrollment information) from the Plan without Participant Authorization only after CSU has amended the Plan and certified that it will limit uses and disclosures of PHI to Plan administrative activities and will otherwise protect PHI as required by the law.

The Plan's certification and Amendment are in Sections 8.03 and 8.04. Other than enrollment information, CSU does not receive, use or disclose any other form of PHI without obtaining the Participant's Authorization for all of its health plans other than the HCRA plan. Therefore, CSU has only amended the HCRA plan to allow for the receipt of PHI from the Plan without Participant Authorization. All HCRA claim information (including formal HCRA claim appeals) should be directed to the Systemwide Human Resources Administration benefits staff unless it is obtained through a Participant Authorization.

This Section 5.03 describes CSU's procedures for using or disclosing PHI for HCRA plan administrative activities without Authorization. In general, CSU will:

- Identify the classes of employees with access to PHI and the categories of information they will use;
- To the extent practical, make reasonable efforts to limit disclosures of and requests for PHI to a Limited Data Set and exclude birth date and zip code data or, if needed, the Minimum Necessary to accomplish the intended purpose;
- Maintain procedures governing the storage of PHI; and
- If feasible, return or destroy PHI received from the Plan, and maintain procedures governing the retention and destruction of PHI not returned or destroyed.

Procedures governing disclosures and requests made on a routine and recurring basis are described in the following charts. For other disclosures and requests, CSU will review each situation on an individual basis by considering the importance of the request or disclosure; the costs of limiting the request or disclosure; and any other factors CSU believes to be relevant. Any uses or disclosures of PHI not included in these tables but permitted to be made without Authorization in the Notice of Privacy Practices (see Section 8.02) should be made upon consultation with the Privacy Official if feasible.

a. Appeals of Adverse Benefit Determinations

CSU staff process final appeals to adverse benefit determinations for the HCRA plan only. Process includes collecting information relevant to benefit determination; review and analysis by the appropriate CSU personnel; documenting decision; corresponding with Participant to apprise them of status and final determination; communicating with Business Associates as appropriate. This is a Payment activity.	
CSU staff permitted access to PHI	<ul style="list-style-type: none"> • Systemwide Human Resources Management
Parties to whom disclosures are permitted	<ul style="list-style-type: none"> • Participant who is the subject of the appeal, and associated individuals as permitted by Section 5.05. • Health care providers involved with treating the Participant • Business Associates (e.g., HCRA claims administrator, etc.) involved in the initial benefit determination. • Business Associates (including HCRA claims administrator, health care benefits consultants, etc.) assisting with review and analysis of the benefit determination and appeal.
Categories of PHI	<ul style="list-style-type: none"> • Information relating to appeals, including: <ul style="list-style-type: none"> – Correspondence regarding benefit determinations. – Documents submitted by the claimant, health care providers, etc. – Benefit determinations of Participants receiving similar services.
Protocols for meeting Minimum Necessary requirement	<ul style="list-style-type: none"> • PHI will be De-identified (e.g., name and location removed) to the extent possible by Business Associates or by HR employees before the claim is forwarded to the Systemwide Human Resources Administration Committee. Further, if complete De-identification isn't possible, reasonable effort will be made to forward only a Limited Data Set of PHI and, if possible, also to exclude birth date and zip code data from the information.
Storage of PHI	<ul style="list-style-type: none"> • Paper records will be maintained in a separate file from employment records (see Section 6.02). • Information will be protected using the procedures in Section 4.02.
Retention/ Destruction	<ul style="list-style-type: none"> • PHI will be maintained for at least 6 years after creation and will then be destroyed.

b. Customer Service

<p>Certain CSU staff assists Participants with various eligibility and claims questions. Questions related solely to enrollment and disenrollment will be processed in accordance with Section 5.02. Process involves intake of questions from Participants, collecting information relevant to question; documenting decision; communicating with Participant to apprise them of status and resolution; communicating with Business Associates and Insurers as appropriate. If the CSU staff is going to be sharing and receiving PHI with the health insurance carriers, HMOs, external EAP vendors and/or HCRA claims administrator, the CSU staff must get a Participant Authorization first. See Section 5.04. This is a Payment activity.</p>	
CSU staff permitted access to PHI	<ul style="list-style-type: none"> • Campus benefits staff • Systemwide Human Resources Administration benefits staff • Chancellor's Office staff involved in benefit administration
Parties to whom disclosures are permitted	<ul style="list-style-type: none"> • Participant who is the subject of a question, and associated individuals as permitted by Section 5.05. • Health care providers involved with treating the Participant • Business Associates (e.g., external EAP vendors, HCRA claims administrator, etc.), HMOs and insurance carriers involved in benefit determinations. • Business Associates (e.g., external EAP vendors, HCRA claims administrator, health care benefits consultants, etc.), HMOs and insurance carriers assisting with review and analysis of benefit determinations.
Categories of PHI	<ul style="list-style-type: none"> • All PHI relevant to the claim.
Protocols for meeting Minimum Necessary requirement	<ul style="list-style-type: none"> • To the extent practical, CSU staff will disclose only a Limited Data Set and exclude birth date and zip code data, or if necessary, the PHI that, in their judgment, is directly relevant to the resolution of the question. • Questions about the scope of requested disclosures should be directed to the appropriate Campus Privacy Contact and the Privacy Official.

Storage of PHI	<ul style="list-style-type: none"> Paper records will be maintained in a separate file from employment records (see Section 6.02). Information will be protected using the procedures in Section 4.02.
Retention/ Destruction	<ul style="list-style-type: none"> PHI will be maintained for at least 6 years after creation and will then be destroyed.

c. Data Analysis

CSU staff may perform plan auditing, rate setting and benefits planning and analysis using claims and appeals information that have been de-identified. No individual claims and appeals information should be used for these purposes for any plan other than the HCRA plan. Business Associates perform claim data collection and warehousing services and provide quarterly reports to CSU for the purpose of performing trending, forecasting, and cost calculations. These are both Health Care Operations activities and Payment activities.	
CSU staff permitted access to PHI	<ul style="list-style-type: none"> Systemwide Human Resources Management benefits staff. Finance Department employees. <i>(They may need only de-identified information)</i>
Parties to whom disclosures are permitted	<ul style="list-style-type: none"> Business Associates involved in data aggregation. Business Associates assisting with review and analysis of data.
Categories of PHI	<ul style="list-style-type: none"> All claims data related to Participants, but excluding any physician notes and underlying claim records.
Protocols for meeting Minimum Necessary requirement	<ul style="list-style-type: none"> To the extent practical, Business Associate will only use a Limited Data Set, and exclude birth date and zip code data, or if necessary, remove all unneeded identifiers (e.g., name, location, ID number) before providing PHI to CSU.
Storage of PHI	<ul style="list-style-type: none"> Information will be protected using the procedures in Section 4.02.
Retention/ Destruction	<ul style="list-style-type: none"> PHI will be maintained for at least 6 years after creation and will then be destroyed.

d. Citations

45 CFR § 164.506

§ 13405(b) of HITECH Act (Title XIII, Subtitle D of the American Recovery and

Reinvestment Act of 2009)

5.04 When Authorizations are Needed

CSU will obtain a Participant's Authorization for any use or disclosure of PHI not identified in Section 5.01, including any uses for employment-related or non-Plan-related purposes. Circumstances in which CSU will obtain a Participant's Authorization include (but are not limited to) the following:

- Customer Service activities (see Section 5.03(b) above) such as helping a participant get a claim paid or obtain preauthorization for a medical procedure.

Authorizations will also be obtained for the use or disclosure of Psychotherapy Notes, except in limited circumstances identified in the HIPAA Privacy Rule. (CSU's Privacy Official will review any request for disclosure of information that may qualify as Psychotherapy Notes on an individual basis, in consultation with the Privacy Official, to determine whether the requirements of the HIPAA Privacy Rule are satisfied.)

PHI will not be used or disclosed on the basis of an Authorization, unless it is verified that the Authorization:

- Has not expired;
- Has not been revoked; and
- Includes all required information.

The requirements for Authorizations are described in Section 8.06.

A copy of each Authorization will be retained for at least six (6) years from the later of the date the Authorization was created or the last date the Authorization was effective.

a. Citations

45 CFR § 164.508

5.05 Disclosure to Participants, Beneficiaries, and Others Acting on Their Behalf

This Section 5.05 describes CSU's procedures for disclosing PHI to Participants, their personal representatives, and family members and others acting on their behalf. Insurers and Business Associates will adopt similar procedures for the PHI they use or disclose for the Plan. Before disclosing any PHI, CSU will verify the identity of the person requesting the information (see Section 4.03).

a. Participants

A Participant's own PHI may be disclosed to the Participant without Authorization.

b. Personal Representatives

A personal representative will be treated as the Participant and the Participant's PHI may be disclosed to the personal representative without Authorization. CSU will make reasonable efforts to limit disclosures with respect to PHI to the information relevant to such personal representation. A person will be treated as a personal representative in accordance with the following table and applicable state law. However, see the discussion following this table for important restrictions on personal representative status.

Participant	Person requesting PHI	Personal representative?
Minor/Adult child	Parent or guardian*	Yes, but must be sure they really are the parents or guardian. Should ask for some type of verification.
Adult	Spouse or other adult	Yes, but must be sure they really are the legal spouse or have legal authority (e.g., court order) or voluntary agreement (e.g., power of attorney). Should ask for some type of verification.
Deceased	Executor or Administrator	Yes, but only upon proof of legal authority (e.g., provisions of a will or power of attorney).

*This includes a person with the legal authority to make health care decisions.

Restrictions Regarding Minor Children

CSU generally will treat the parent (or guardian or other person acting in the place of a parent) of a minor child as the child's personal representative, in accordance with applicable state law.

Restrictions Regarding Abuse or Endangerment

CSU may elect not to treat a person as a Participant's personal representative if, in the exercise of professional judgment, CSU decides that it is not in the best interest of the Participant because of a reasonable belief that:

- The Participant has been or may become subject to abuse, domestic violence, or neglect by the person; or
- Treating the person as a personal representative could endanger the Participant.

A Participant may request that the Plan limit communications with a personal representative by submitting a request for Confidential Communications (see Section 6.05).

c. Others Acting on a Participant's Behalf

The HIPAA Privacy Rule provides discretion to disclose a Participant's PHI to any individual without Authorization if necessary for Payment or Health Care Operations. This can include disclosures of a Participant's PHI to the Participant's family members. In making these disclosures, CSU will make reasonable efforts to limit disclosures to the Minimum Necessary to accomplish the intended purpose.

In certain additional cases, PHI can be disclosed without Authorization to a Participant's family members, friends, and others who are not personal representatives, if any of the following conditions applies:

- Information describing the Participant's location, general condition, or death is provided to a family member or other person responsible for the Participant's care (including PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts);
- PHI is disclosed to a family member, close friend or other person identified by the Participant who is involved in the Participant's care or Payment for that care, and the Participant had the opportunity to agree or object to the disclosure; or
- PHI is disclosed to a family member or friends involved in the Participant's care and it is impossible (due to incapacity or emergency) to obtain the Participant's agreement.

d. Citations

45 CFR § 164.502(g)

45 CFR § 164.510

5.06 List of Legally Required Uses, Public Health Activities, Other Situations Not Requiring Authorization

The Plan, its Insurers and Business Associates will, without obtaining a Participant's Authorization or any Plan Amendment, use and disclose PHI if required by law, for certain public health purposes, and in other similar situations, described in the following chart below.

All such requests should be immediately forwarded to the Privacy Official.

Purpose for disclosure	Permissible disclosures of PHI
Workers' compensation	<ul style="list-style-type: none"> Includes disclosures of PHI to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with such laws.
Necessary to prevent or lessen serious threat to health or safety	<ul style="list-style-type: none"> Includes disclosures of PHI to a person or persons if made under good faith belief that releasing PHI is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety if made to someone reasonably able to prevent or lessen the threat (including disclosures to the target of the threat). Includes disclosures of PHI to assist law enforcement officials in identifying or apprehending an individual because the individual has made a statement admitting participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody.
Public health activities	<ul style="list-style-type: none"> Includes disclosures of PHI authorized by law to persons who may be at risk of contracting or spreading a disease or condition. Includes disclosures of PHI to public health authorities to prevent or control disease and to report child abuse or neglect. Includes disclosures of PHI to the FDA to collect or report adverse events or product defects.
Victims of abuse, neglect, or domestic violence	<ul style="list-style-type: none"> Includes disclosures of PHI to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or

Purpose for disclosure	Permissible disclosures of PHI
	domestic violence, as required by law or if the subject of the PHI agrees or the Plan believes disclosure is necessary to prevent serious harm to the individual or potential victims; the Plan will notify the individual that is the subject of the disclosure if it won't put the individual at further risk.
Judicial and administrative proceedings	<ul style="list-style-type: none"> Includes disclosures of PHI in response to a court or administrative order; and disclosures in response to a subpoena, discovery request or other lawful process (the Plan is required to notify the individual that is the subject of the request for PHI of the request, or to receive satisfactory assurance from the party seeking the PHI that efforts were made to notify the individual that is the subject of the request for PHI or to obtain a qualified protective order concerning the PHI).
Law enforcement purposes	<ul style="list-style-type: none"> Includes disclosures of PHI to law enforcement officials as required by law or pursuant to legal process, or to identify a suspect, fugitive, witness or missing person. Includes disclosures of PHI about a crime victim if the individual that is the subject of the PHI agrees or if disclosure is necessary for immediate law enforcement activity. Includes disclosures of PHI regarding a death that may have resulted from criminal conduct and disclosures to provide evidence of criminal conduct on the Plan's premises.
Decedents	<ul style="list-style-type: none"> Includes disclosures of PHI to a coroner or medical examiner to identify the deceased or to determine the cause of death, and to funeral directors to carry out their duties.
Organ, eye, or tissue donation	<ul style="list-style-type: none"> Includes disclosures of PHI to organ procurement organizations or other entities to facilitate cadaveric organ, eye, or tissue donation and transplantation.
Research purposes	<ul style="list-style-type: none"> Includes disclosures of PHI subject to approval by institutional or privacy boards, and subject to certain assurances and representations by researchers regarding necessity of using PHI and treatment of PHI during a research project.
Health oversight activities	<ul style="list-style-type: none"> Includes disclosures of PHI to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, compliance with regulatory programs, or civil rights laws.
Specialized government functions	<ul style="list-style-type: none"> Includes disclosures of PHI of individuals who are Armed

Purpose for disclosure	Permissible disclosures of PHI
	<p>Forces personnel or foreign military personnel under appropriate military command authority.</p> <ul style="list-style-type: none">• Includes disclosures to authorized federal officials for national security or intelligence activities.• Includes disclosures to correctional facilities or custodial law enforcement officials about inmates.
Department of Health and Human Services (HHS) Investigations	<ul style="list-style-type: none">• Includes disclosures of PHI to HHS to investigate or determine the Plan's compliance with the HIPAA Privacy Rule.

5.07 Use and Disclosure of De-Identified Information and Data Use Agreements

Health information can be used without complying with the limits in this Manual if names, Social Security numbers and other data are removed so there is no reasonable basis to believe it can be used to identify a person. A Plan may choose to de-identify PHI and then use it without written Authorization from the persons to whom it pertains. A Plan can also remove most identifying data and disclose it without Authorization for selected purposes if the recipient agrees to protect the data through a Data Use Agreement.

The following are examples of health information that has been de-identified:

- There was a medical claim for \$5,000 last month;
- There were 500 people enrolled in the HCRA plan last month.

Insurers and Business Associates acting on behalf of the Plan will adopt procedures for applying these De-identification rules and entering into Data Use Agreements. CSU's procedures are described in this Section.

a. De-Identified Information

To de-identify Plan information, the specific data in the following list will be removed. However, if CSU knows that the information could still be used to identify a person, it will be protected as PHI.

- | | | |
|--|---|--|
| • Names; | • Geographic identifiers smaller than a state, including street address, city, county, precinct, and zip code. <i>The first three (3) numbers of the zip code can be used if more than 20,000 people are in any combination of zip codes with the same first three (3) numbers;</i> | • Device identifiers and serial numbers; |
| • Social Security number; | | • Web Universal Resource Locators (URLs); |
| • Specific dates such as dates of birth and death, and admission/discharge dates. <i>The Plan can use the year of the event, except for the birth years of persons over age eighty-nine (89)</i> | • Account numbers; | • Internet Protocol (IP) address numbers; |
| • Telephone numbers; | • Certificate/license numbers; | • Biometric identifiers (e.g., finger, iris, or voice prints); |
| • Fax numbers; | • Vehicle identifiers (serial | • Full-face photographic and any comparable images; and |
| • E-mail addresses; | | |

- Medical record numbers; numbers or license plate numbers);
- Health plan beneficiary number;
- Any other unique identifying numbers or characteristics or codes, including a particular subsidiaries, divisions or work locations.

The Plan can retain a code (or other method) for re-identifying a person's information in the future, if the identification mechanism will not be used or disclosed and cannot be translated so as to identify the person. If the health information is re-identified, the Plan will treat it as PHI subject to this Manual.

As an alternative to removing all the items above, a case-by-case decision can be made about how much data needs to be removed in order to de-identify information. To do so, a written statement and analysis must be obtained from an appropriate expert in statistics and information de-identification. The statement must conclude that the risk is very small that the information could be used (alone or in combination with other information) to identify an individual.

b. Data Use Agreements

It is very unlikely that CSU would ever need to use a data use agreement. This section has been included in the rare case that CSU decides to use such an agreement.

In limited circumstances, PHI may be disclosed without Authorization under a data use agreement. This type of disclosure is permitted upon receipt of a request for health information needed for research purposes or public health activities, if the request fails to meet the requirements in Section 5.06. The same procedures can be used to disclose PHI without Authorization for certain types of Health Care Operations not specifically described in Section 5 or the Definitions.

For example, a data use agreement may be used to disclose information for research that has not been approved by a review board; for public health activities undertaken by private organizations instead of public health authorities; and for Health Care Operations by providers or other health plans that do not have a prior or current relationship with the subject of the PHI.

To disclose PHI without Authorization in these circumstances, the Plan must:

- Create a “Limited Data Set” by removing most of the identifying data listed in the table in Section 5.07(a). If all of the data is removed, the information is de-identified and can be used or disclosed without restriction. Key dates (birth date, admission/discharge date, date of death) and certain geographic information, such as city and zip code, may be retained; and
- Receive assurances from the recipient of the data that it will protect the information through a data use agreement. The agreement must establish the permitted uses and disclosures of the information, limit who can use or receive it, and promise that the recipient will safeguard the information.

CSU will review each request for disclosure of information that may qualify for data use agreements on an individual basis, in consultation with the Privacy Official, to determine whether the requirements in the HIPAA Privacy Rule are satisfied.

c. Citations

45 CFR § 164.514

45 CFR § 164.502(d)

5.08 Reporting Improper Access, Uses and Disclosures

If PHI is accessed, used, or disclosed in any way not permitted by the provisions of this Manual, then such access, use, or disclosure is improper (called a “breach”). If a PHI breach occurs, CSU must investigate facts about the incident, assess whether and who must be notified of the event, and evaluate alternative ways to prevent a similar occurrence in the future (see Section 6.05). Federal law protects staff from any type of retaliation for reporting any incident if the staff member has a good faith belief that a HIPAA violation has occurred. CSU staff must report all PHI breaches as soon as they are discovered. CSU staff will report both confirmed breaches and suspected incidents for which there is a reasonable belief that a breach has occurred or is occurring.

a. How to Report a PHI Breach

An CSU workforce member will complete a Breach Incident Report Form (Section 10.09(a)) and e-mail it or send it by facsimile to the Plan’s Breach Contact listed on the Form 10.09(a). In the case of an ongoing incident or series of incidents, rather than a completed event that occurred in the past, the CSU workforce member will immediately contact the Breach Contact and communicate the information required on the Form 10.09(a).

b. What Information to Include in a Breach Report

Workforce members must complete all sections of the Form 10.09(a) as fully as possible. If the workforce member is uncertain of the exact number of individuals whose PHI was used or disclosed in the incident, a reasonable estimate should be provided.

c. When to Submit a Breach Report

In the case of confirmed or suspected PHI breach incidents that are not ongoing, workforce members are to complete the Form 10.09(a) within two business days of discovering the incident.

If the breach is, or is suspected of being, a continuing type of event rather than one which has occurred wholly in the past, CSU workforce members should contact the Breach Contact as soon as the member reasonably believes that a continuing incident is occurring.

d. Documentation

CSU will maintain all Breach Incident Report Forms submitted to the Breach Contact for a period of six (6) years.

e. Citations

45 CFR Part 164, Subpart D

6. Individual Rights

6.01 Overview

6.02 Inspect and Copy PHI

6.03 Amend PHI

6.04 Restricted Use of PHI

6.05 Confidential Communications

6.06 Accounting of Non-Routine Disclosures

6.01 Overview

The HIPAA Privacy Rule provides individuals with certain rights associated with their PHI that the Plan (and all other Covered Entities) must follow. These include the rights to:

- Access, inspect, and copy certain PHI within a Designated Record Set (see Section 6.02);
- Request the Amendment of their PHI in a Designated Record Set (see Section 6.03);
- Request restriction of the use and disclosure of their PHI (see Section 6.04);
- Request the use of alternative means or alternative locations for receiving communications of their PHI (see Section 6.05); and
- Request an accounting of PHI disclosures (see Section 6.06).

Section 11.03 identifies the contact persons for processing Participants' requests to exercise these rights.

The health insurance carriers, HMOs, external EAP vendors or the HCRA claims administrator have most of the PHI held in Designated Record Sets for the Plan. CSU has very limited Designated Record Sets. The Designated Record Sets held by CSU do not include eligibility and enrollment information (regardless of who provided it to CSU), information received by CSU from the employee directly, and information received by CSU from the health insurance carriers, HMOs, external EAP vendors, and/or HCRA claims administrator with a Participant Authorization. The PHI that is held by CSU in a Designated Record Set is described on in Section 6.02(a) below. All Designated Records Sets for CSU will be held by the Systemwide Human Resources Administration benefits staff and none of the campuses should have any Designated Record Sets.

All Participant requests (other than requests for restrictions or requests for alternative means or locations for receiving communications of PHI) that pertain to CalPERS medical, dental or vision coverage should be directed to the applicable HMO or insurance carrier. In other words, please have the Participant contact the HMO or insurance carrier directly since CSU does not maintain Designated Record Sets for those coverages.

For all other requests, the Campus Privacy Contact or Privacy Official will have the Participant fill out the applicable Form from Section 11.07 and all such Forms will be forwarded to the Privacy Official. The Privacy Official will respond to all such requests.

6.02 Inspect and Copy PHI

a. Participant's Right

A Participant has the right to access, inspect, and copy his or her PHI within a Designated Record Set for as long as the PHI is maintained in the Designated Record Set. The Plan must generally honor these rights, except in certain circumstances the Plan may deny the right to access. The Plan may provide a summary or explanation of the PHI instead of access or copies, if the Participant agrees in advance and pays any applicable fees.

Copies of Electronic Health Records. Effective February 17, 2010, a Participant may request an electronic copy of his PHI (or summary or explanation) if it is maintained in an Electronic Health Record. A Participant may also request that such PHI be sent to another entity or person, so long as that request is clear, conspicuous and specific. The Plan may charge the Participant a reasonable fee for these copies that is no greater than the Plan's labor costs. The CSU does not hold Electronic Health Records on behalf of the group health plans.

A Designated Record Set is a group of records that the Plan maintains for enrollment, Payment, claims adjudication, case management or medical management, or that the Plan uses, in whole or in part, to make decisions about Participants. Although a Designated Record Set includes the Plan's enrollment and Payment information, it does not include CSU's enrollment and payment records, information received by CSU from the employee directly, and information by CSU received from the health insurance carriers, HMOs, external EAP vendors, and/or HCRA claims administrator with a Participant Authorization. The Plan will require Business Associates to identify Designated Record Sets that they maintain and to make them available for inspection and copying. CSU maintains the following Designated Record Sets, which are available to be inspected or copied:

- HIPAA File (e.g., the Participant files that contain HCRA claim appeals records, Participant Authorizations, other HIPAA Participant PHI requests).

b. Processing a Request

The Plan is responsible for receiving and processing requests for access, inspection, and copying of PHI maintained in Designated Record Sets. If the Plan does not maintain the PHI that is the subject of the Participant's request but knows where it is maintained, the applicable Campus Privacy Contact will inform the Participant where to direct his or her request. The Plan will develop procedures with Business Associates to coordinate the inspection of Designated Record Sets in the Business Associates' custody.

The Campus Privacy Contacts (see Section 11.03) will be responsible for taking the initial requests

from Participants and having Participants complete the applicable Form. If the request relates to a Designated Record Set maintained by the CalPERS medical, dental or vision insurance carriers or HMOs, the Campus Privacy Contact should direct the Participant to the applicable company. If the request relates to a Designated Record Set maintained by CSU, the external EAPs or the HCRA claims administrator, the Campus Privacy Contact should immediately forward it to the Privacy Official after the Participant has completed the applicable Form. If the Campus Privacy Contact is unsure who maintains the Designated Record Set, the Campus Privacy Contact should ask the Privacy Official for guidance.

Requests for access, inspection, and copying of PHI must be submitted on the Request for Access Form [\(Section 11.08\(a\)\)](#) and sent to the applicable Campus Privacy Contact who will forward the form to the Privacy Official.

The Privacy Official will respond to a Participant's request within thirty (30) days of the receipt of the request. If the requested PHI is maintained offsite, the Privacy Official will respond within sixty (60) days of the request. If the Privacy Official is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which the Privacy Official expects to address the request.

c. Accepting a Request to Access, Inspect, or Copy

If the Privacy Official accepts the request, a copy of Form 11.08(a) indicating that the request has been accepted will be sent to the Participant and access will be provided within the thirty/sixty (30/60) day timeframe. A fee will be charged to the Participant for copying and mailing, based on the actual cost. Form 11.08(a) will inform the Participant of the fees in advance, and give the Participant an opportunity to withdraw the request if he or she does not agree to the fees.

d. Denying a Request to Access, Inspect, or Copy (Where Participant has Right to Review)

If the Privacy Official denies a request, a copy of Form 11.08(a) indicating that the request has been denied will be sent to the Participant within the thirty/sixty (30/60) day timeframe. Form 11.08(a) will indicate whether the Participant has the right to a review of the denial.

The Participant has the right to have the denial reviewed if the Privacy Official denies access to PHI for any of the following reasons:

- A licensed health care professional determines that the access is reasonably likely to endanger the life or physical safety of the Participant or another person;
- The PHI contains information about another person and a licensed health care professional

determines that the access is reasonably likely to cause substantial harm to the other person; or

- The request is made by a personal representative, and a licensed health care professional determines that providing access to the personal representative is reasonably likely to cause substantial harm to the Participant or another person.

If the Privacy Official denies access on the basis of the risk of harm identified by a licensed health care professional, the Participant has the right to have the denial reviewed by a different licensed health care professional. The Privacy Official will promptly refer a request for review to a licensed health care professional who did not participate in the original denial decision. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access. The Privacy Official will provide or deny access in accordance with the determination of the reviewing official.

If the Privacy Official denies access to any PHI, the Plan will, to the extent possible, continue to provide access to other PHI for which there are no grounds to deny access.

e. Denying a Request to Access, Inspect, or Copy (Where Participant has NO Right to Review)

If the Privacy Official denies a request, a copy of Form 11.08(a) indicating that the request has been denied will be sent to the Participant within the thirty/sixty (30/60) day timeframe. The copy will indicate whether the Participant has the right to a review of the denial.

The Participant has no right to have a denial reviewed if the Privacy Official denies a request to access, inspect, or copy PHI, for any of the following reasons:

- The PHI is Psychotherapy Notes;
- The PHI was compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative proceedings;
- The Plan maintains that the PHI is also subject to the Privacy Act (5 U.S.C. § 552a), and the Privacy Act allows the denial of access;
- The Plan received the PHI from someone other than a health care provider under a promise of confidentiality, and providing access to the PHI would be reasonably likely to reveal the source; or
- The Plan has temporarily suspended access to PHI created for research involving Treatment, if the Participant agreed to the suspension of access when agreeing to participate in the research.

f. Form for Denial

If the request for access is denied, the Privacy Official will within the timeframes, provide a written denial (see Section 11.08(a)) to the Participant in plain language which contains:

- The basis for the denial;
- A statement of the individual's review rights, if any; and
- A description of how the individual may complain to the Plan, pursuant to the complaint procedure in Section 7.03, or to HHS.

g. Documenting Requests

All requests, acceptances, and denials of PHI will be documented and retained for a period of at least six (6) years.

h. Citations

45 CFR § 164.524

§ 13405(e) of HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009)

6.03 Amend PHI

a. Participant's Rights

A Participant has the right to request that the Plan amend his or her PHI in a Designated Record Set. The Plan must generally honor these rights, except in certain circumstances. When the Plan amends PHI, it must communicate the Amendment to other persons to whom it has disclosed the PHI as described in Section 6.03(c). The Plan will require Business Associates to make Designated Record Sets that they maintain available for Amendment requests.

b. Processing a Request

The Plan is responsible for receiving and processing requests for Amendments to PHI. All requests for Amendment to Designated Record Sets held by CSU, the HCRA claims administrator, or the external EAPs must be forwarded to the Privacy Official immediately by the Campus Privacy Contacts after the Campus Privacy Contact has the Participant complete the applicable Form. However, if the request relates to a Designated Record Set held by the CalPERS medical, dental or vision health insurance carriers or HMOs, the Campus Privacy Contact should refer the Participant to the applicable company. Requests must be submitted on the Request to Amend Form (see Section 11.08(b)) and sent to the applicable Campus Privacy Contact who will forward the Form to the Privacy Official. The Plan will develop procedures with Business Associates to coordinate the right to request Amendment of Designated Record Sets in the Business Associates' custody.

The Privacy Official will respond to a Participant's request within sixty (60) days after receipt. If the Privacy Official is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which the Privacy Official expects to address the request.

c. Amending PHI and Notifying Others

If the Privacy Official accepts a request for Amendment, in whole or in part, a copy of Form 11.08(b) indicating that the request has been accepted will be sent to the Participant within the sixty (60) day time frame. The Privacy Official will amend the PHI appropriately, and make reasonable efforts to inform and provide the Amendment to:

- Persons identified by the Participant as having received the PHI that is to be amended; and
- Persons, including Business Associates, who the Plan knows have the PHI that is the subject of

the Amendment and who may have relied, or could foreseeably rely, on the information to the detriment of the Participant.

d. Denying an Amendment

If the Privacy Official denies the request for Amendment, in whole or in part, a copy of Form 11.08(b) indicating that the request was denied will be sent to the Participant within the sixty (60) day time frame. The Privacy Official may deny a request to amend a Participant's PHI if he or she determines that the PHI:

- Was not created by the Plan (unless the Participant provides a reasonable basis to believe that the creator of the PHI is no longer available to amend the PHI);
- Is not part of the Designated Record Set;
- Is not available for inspection under the HIPAA Privacy Rule; or
- Is accurate and complete.

If the Privacy Official denies the request, it will permit the Participant to submit a statement of disagreement and the basis for the disagreement, limited to five (5) pages. In response, the Privacy Official may provide a rebuttal statement and send a copy to the Participant.

The Privacy Official will attach to each Designated Record Set that is subject to the request a completed copy of Form 11.08(b) (including any attached disagreement statements and rebuttals) indicating the denial of the Amendment request.

When the Plan makes subsequent disclosures of the disputed PHI, a copy of Form 11.08(b) (or a summary of the information included on Form 11.08(b)) will be attached to the PHI disclosed in the following circumstances:

- When the Participant has submitted a statement of disagreement;
- When the Participant has so requested.

e. Documenting Requests

All requests, acceptances, denials, and supporting statements regarding Amendment of PHI will be documented and retained for a period of at least six (6) years.

f. Citations

45 CFR § 164.526

6.04 Restricted Use of PHI

a. Participant's Rights

A Participant has the right to request that the Plan restrict the use and disclosure of his or her PHI. The Plan is not required to agree to a restriction, but it must abide by an agreed to restriction except in certain circumstances. The Plan will require Business Associates to make PHI that they maintain available for restriction requests.

b. Receiving a Request

The Plan is responsible for processing requests for restricted use of PHI. The Plan has assigned this responsibility to the Privacy Official. Requests must be submitted on the Request for Restricted Use Form (see Section 10.08(c)) and sent to the Privacy Official. The Plan will develop procedures with Business Associates to coordinate the restricted use of PHI in the Business Associates' custody.

c. Processing a Request

The Privacy Official will not agree to any requests for restricted use of PHI except to a restriction request meeting the conditions of "Out-of-Pocket Payments" below.

Out-of-Pocket Payments. The Privacy Official will agree to restrict disclosure to a health plan for purposes of carrying out payment or health care operations if the request relates to PHI for a health care item or service for which the provider has already been paid in full out-of-pocket. (For example, the Privacy Official would agree *not* to forward a provider's claim for payment to another health plan for coordination of benefits purposes if the Participant has already paid out of his own pocket the full amount to the provider for the service rendered.)

Procedures. The Privacy Official will provide notice of the approval or denial of the request.

- If approved, a copy of Form 10.08(c) indicating that the request has been approved will be sent to the Participant and to each Business Associate that has access to that Participant's PHI.
- If denied, a copy of Form 10.08(c) indicating that the request has been denied will be sent to the Participant.

d. Documenting Requests

All restricted use of PHI requests will be documented and retained for a period of at least six (6) years.

e. Citations

45 CFR § 164.522(a)

§ 13405(a) of HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009)

6.05 Confidential Communications

a. Participant's Rights

A Participant has the right to request that the Plan use alternative means or alternative locations to communicate PHI to the Participant. The Plan must accommodate reasonable requests if the Participant clearly states that the disclosure of the PHI by the usual means could endanger the Participant. The Plan will require Business Associates that maintain PHI to reasonably honor a Participant's request for alternative means or locations to communicate the PHI to the Participant.

b. Processing a Request

The Plan is responsible for receiving and processing requests for Confidential Communication of PHI. All requests for confidential communications should be immediately forwarded to the Privacy Official by the Campus Privacy Contact, even if the request relates to a Designated Record Set held by the CalPERS medical, dental or vision health insurance carriers or HMOs. Requests must be submitted on the Request for Confidential Communications Form (see Section 11.08(d)) and sent to the applicable Campus Privacy Contact who will forward it to the Privacy Official. The Plan will develop procedures with Business Associates to coordinate the Confidential Communications of PHI in Business Associates' custody.

The Privacy Official will determine whether to approve or deny the request on the basis of its reasonableness. Reasonableness will be determined on the basis of the administrative difficulty in complying with the request and in consultation with the Privacy Official, as needed. If the payment of benefits is affected by this request, the Plan may also deny this request unless the Participant contacts the Privacy Official to discuss alternative payment means.

The Privacy Official will provide notice of the decision to approve or deny the request.

- If approved, a copy of Form 11.08(d) indicating that the request has been approved will be sent to the Participant and each Business Associate that has access to that Participant's PHI.
- If denied, a copy of Form 11.08(d) indicating that the request has been denied will be sent to the Participant.

c. Documenting Requests

All requests for Confidential Communication of PHI will be documented and retained for a period of

at least six (6) years.

d. Citations

45 CFR § 164.522(b)

6.06 Accounting of Non-Routine Disclosures

a. Participant's Rights

A Participant has the right to request an accounting of PHI disclosures made under Section 5.06 and disclosures not otherwise permitted by Section 5. However, an accounting is not available to the Participant in circumstances involving:

- National security or intelligence purposes;
- Correctional institutions or law enforcement officials;
- Limited Data Sets; and
- Disclosures occurring before the compliance date for the Covered Entity.

The Participant can request that the accounting include disclosures made on or after the later of:

- April 14, 2003 for all the group health plans sponsored by CSU other than the external EAPs and the HCRA plan.
- April 14, 2004 for the external EAP and HCRA plans.
- The date that is six (6) years prior to the date of the request.

The Plan will require Business Associates that maintain PHI to reasonably honor a Participant's request for accountings of PHI disclosures.

b. Processing a Request

The Plan is responsible for receiving and processing requests for an accounting of PHI disclosures. All accounting requests regarding Designated Record Sets held by CSU, the HCRA claims administrator, or the external EAP should be immediately forwarded to the Privacy Official by the Campus Privacy Contact after the Campus Privacy Contact has the Participant complete the applicable Form.

However, if the request relates to a Designated Record Set held by the CalPERS medical, dental or vision health insurance carriers or HMOs, the Campus Privacy Contact should refer the Participant to the applicable company. Requests must be submitted on the Request for Accounting of Non-Routine Disclosures Form (see Section 11.08(e)) and sent to the applicable Campus Privacy Contact who will forward the Form to the Privacy Official. The Participant must indicate whether the requested accounting is for disclosures made within the past six (6) years or some shorter time period. The Plan

will develop procedures with Business Associates that maintain PHI to coordinate the requests for accounting of PHI disclosures.

The Privacy Official generally will respond to a request for an accounting within sixty (60) days after receipt. If the Privacy Official is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which the Privacy Official expects to address the request.

The Privacy Official will send a copy of Form 11.08(e) to the Participant, with the accounting of PHI disclosures attached.

The Privacy Official will provide a Participant with one accounting in any twelve (12)-month period free of charge. A reasonable fee will be charged for subsequent accountings within the same twelve (12)-month period.

The Privacy Official may temporarily suspend a Participant's right to receive an accounting of disclosures to:

- A health oversight agency for health oversight purposes; or
- A law enforcement official for law enforcement purposes,

If the agency or official informs the Privacy Official or the Plan in writing that the accounting would be reasonably likely to impede the agency's activities, and if it indicates the time for which the suspension is required.

The Privacy Official will suspend a Participant's right to receive an accounting of these disclosures for up to thirty (30) days upon an oral request from the agency or official.

c. Content of the Accounting

The Privacy Official will include the following information in an accounting of PHI disclosures:

- Date of disclosure;
- Name (and address, if known) of person or entity that received the PHI;
- Brief description of the PHI disclosed; and
- An explanation of the purpose of the disclosure or a copy of the request for disclosure.

The HIPAA Privacy Rule permits an abbreviated accounting of multiple PHI disclosures made to the same person or entity for a single purpose, and of certain disclosures for research purposes.

d. Documenting Requests

All requests for accounting of PHI disclosures will be documented and retained for a period of at least six (6) years.

e. Citations

45 CFR § 164.528

7. Risk Management Activities

7.01 Overview

7.02 Training

7.03 Complaints

7.04 Sanctions

7.05 Mitigation

7.06 Document Retention

7.01 Overview

The Plan is participating in certain risk management activities to ensure compliance with the HIPAA Privacy Rule including:

- Workforce training on the Policies and Procedures for use, disclosure and general treatment of PHI (see Section 7.02);
- Developing a complaint process for individuals to file complaints about the Plan's Policies and Procedures, practices, and compliance with the HIPAA Privacy Rule (see Section 7.03);
- Subjecting CSU employees who violate CSU's HIPAA privacy policies and procedures to appropriate disciplinary actions (see Section 7.04);
- Mitigating damages known to the Plan resulting from improper use or disclosure of PHI (see Section 7.05); and
- Retaining copies of its Policies and Procedures, written communications, and actions or designations (see Section 7.06).

Sections 7.02 through 7.06 describe the Procedures developed by CSU.

7.02 Training

HIPAA generally requires Covered Entities to provide training to all current and future workforce members under their direct control on the use, disclosure, and general treatment of PHI. Since the Plan itself has no workforce members, CSU will train its workforce members to ensure that it meets its obligations under this Manual (including limiting the use, disclosure of PHI as required under Section 5). The Privacy Official or the Campus Privacy Contacts will coordinate the training for the CSU. Business Associates and Insurers will separately engage in training activities as needed to ensure they meet their responsibilities under the HIPAA Privacy Rule and Business Associate Agreements (as applicable).

a. When Training will Occur

Workforce members of CSU who will have access to PHI will receive privacy training. CSU will also retrain appropriate members of the workforce following a material change in the Plan's Policies and Procedures. The retraining will occur within a reasonable period of time after the Plan changes its Policies and Procedures.

b. Contents of Training

Workforce training on the use and disclosure of PHI will address the protection, permissible disclosures, and general treatment of PHI.

The following topics are to be covered in the training:

Training topics
The definition of PHI
The Plan's processes for using and disclosing PHI (include applicable state-specific requirements)
The Plan's processes for handling Authorizations
How to respond to requests for PHI from various parties (family members, law enforcement, etc.)
The Plan's physical safeguard procedures for protecting PHI
The identification of the Privacy Official and the Campus Privacy Contacts and their duties and contact information
The identification of Business Associates
An explanation of the Plan's internal complaint procedures

Training topics
How to respond when a violation of the HIPAA Privacy Rule or the Plan's Policies and/or Procedures occurs, including timely action to report any discovery of an improper use or disclosure of PHI, to log breach incidents, to notify required parties about such incidents and take mitigating action, as applicable
The possible sanctions if a workforce member violates the HIPAA Privacy Rule or the Plan's Policies and Procedures

In addition to this Manual, HIPAA information and training materials are contained on the CSU Employee Benefits Program web-site: <http://www.calstate.edu/benefits/healthcare.shtml> and the Systemwide Professional Development website: <http://centralstationu.calstate.edu/howthingswork/>. Employees who will have access to PHI should also be familiarized with the information and materials on the web-site.

c. Documentation

Documentation of privacy training will be maintained by the Privacy Official for system-wide privacy training and by the Campus Privacy Contacts for campus specific privacy training for at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

The documentation of privacy training will include:

Description of documentation
The forum used to train the workforce, including information on whether training is through personal instruction, web-based instruction, individual study, etc.
Information on the training presentation, including the name of the training program, its location and date, the workforce groups attending, etc.
A description and a copy of the training materials.
Information on the presenter including background, qualifications, contact information, etc.
Training attendance records, including directions given to each training location on required information for such records
Evaluation summaries of the training course, if applicable

The Privacy Official may document the above information separately for different offices, locations, or workforce groups, as necessary.

d. Citations

45 CFR § 164.530(b)

7.03 Complaints

The Plan is required to create a process for persons to file complaints about the Plan's Policies and Procedures, practices, and compliance with the HIPAA Privacy Rule. This Section describes the complaint process for self-funded Plan benefits (i.e., the HCRA plan). The health insurance carriers, HMOs and external EAP vendors will develop procedures to process complaints about insured and EAP benefits as required under the HIPAA Privacy Rule.

a. Filing Complaints

Complaints should be filed by contacting the Privacy Official in writing and such written document should include a description of the nature of the particular complaint. The Privacy Official will handle all complaints.

b. Processing Complaints and Complaint Resolution

The Privacy Official will review the complaint, address the situation, consult with the proper individuals (if necessary), and attempt to come to an appropriate resolution of the complaint.

The resolution will depend on the particular facts and circumstances of the complaint. Examples of complaint resolution include:

- Educating the individual about the Plan's Policies and Procedures or practices;
- Coordinating with the Privacy Official regarding complaints alleging use or disclosure of PHI in violation of the Plan's Policies and Procedures;
- Implementing changes in the Plan's Policies and Procedures or practices;
- Providing additional training for workforce members on the Plan's Policies and Procedures, the HIPAA Privacy Rule, or other applicable laws or regulations;
- Discussing a complaint with the relevant parties and, if necessary, imposing sanctions on individuals who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule; and
- Issuing new workforce communication materials or a revised Privacy Notice regarding the Plan's Policies and Procedures.

If, at any time, an individual wants to know the status of his or her complaint, he or she should contact

the Privacy Official.

Once the Privacy Official has resolved a complaint, he or she will contact the individual who filed the complaint and discuss the resolution or will send a written or electronic communication to the individual who filed the complaint explaining the resolution.

c. Documentation

CSU will maintain a record of the complaints and a brief explanation of their resolution, if any, for a period of at least six (6) years.

d. Citations

45 CFR § 164.530(d)

7.04 Sanctions

Covered Entities are required to design a system of written disciplinary policies and sanctions for workforce members who violate the HIPAA Privacy Rule. Since the Plan itself has no workforce members CSU will implement procedures to apply sanctions against its workforce members who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule. Business Associates and Insurers will take whatever steps are required to ensure their compliance with the HIPAA Privacy Rule and Business Associate Agreements (as applicable).

a. Determining Sanctions

Sanctions for violations of CSU's HIPAA privacy policies and procedures will be determined by CSU in accordance with its employment policies and procedures, applicable employment agreements and applicable collective bargaining agreements. CSU will not apply sanctions against workforce members who refuse to follow a policy or procedure that they believe, in good faith, violates the HIPAA Privacy Rule, if the refusal is reasonable and does not involve a disclosure of PHI. In addition, CSU will not apply sanctions against workforce members who file a complaint with any entity about a privacy violation.

b. Documentation

CSU will document in writing (or in an electronic medium) all sanctions it applies. CSU will retain the documentation of any sanctions it applies for at least six (6) years. Both the Privacy Official and Campus Privacy Contacts will maintain records of such sanctions in a designated file and in the applicable employees' personnel files.

c. Citations

45 CFR § 164.530(e)

7.05 Mitigation of PHI Breaches

The Plan is required to mitigate any harmful effects that it knows have resulted from improper access, use, or disclosure (a breach) of PHI in violation of the Plan's Policies and Procedures or the HIPAA Privacy Rule. To meet this obligation, the Plan will coordinate with and require Business Associates to mitigate, to the extent practicable, any harmful effects from breaches of PHI known to them. Insurers are also required to mitigate such harmful effects under HIPAA.

The Plan's Privacy Official will conduct, or direct others in the performance of, the mitigation activities.

a. Investigating Reported Breaches Originating from CSU

The Plan's Privacy Official (or his or her designee) will review all Forms 10.09(a) submitted for evaluation and timely take appropriate steps to learn relevant facts about the incident and apply corrective measures, including:

Verify there was a problematic access, use or disclosure of PHI and confirm that no exception under the Privacy Rule would permit it;

- Interview relevant workforce members to learn about circumstances surrounding the incident;
- Review manual logs, electronic logs, closed circuit television tapes and/or other feasible references to determine the source(s) of the breach if that is unknown;
- Conclude whether an impermissible access, use, or disclosure occurred (or is reasonably believed to have occurred), how it occurred and, in coordination with the Security Official, identify corrective steps needed to prevent a similar incident from reoccurring (which may include additional training for workforce members and applying sanctions against workforce members in accordance with Section 6.04); and
- Begin completion of the Breach Incident Log (Form 10.09(b)) capturing the above facts and conclusions.

b. Assessing Whether the Incident Requires CSU to Send Breach Notices

The Plan has an affirmative duty under HIPAA's Breach Notice Rule to send affected individuals a notice about impermissible accesses, uses and disclosures of their PHI unless an exception to the breach notice requirement applies.

The Privacy Official (or his or her designee) will initially assess whether an exception to the notice duty applies to the incident under the Breach Notice Rule, including:

The affected data was in a “secured” format at the time of the incident (that is, a format deemed by HHS to make the PHI unusable, unreadable, or indecipherable to unauthorized persons – as outlined in then-applicable HHS guidelines found at <http://www.hhs.gov/ocr/privacy> or other successor website);

- The amount of PHI accessed, used or disclosed was limited to those elements allowed in a Limited Data Set, and also excluded dates of birth and zip code data;
- The incident consisted of the unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the Plan or a Business Associate, and the acquisition, access or use was made in good faith and within the scope of authority and did not result in further use or disclosure that is disallowed under the Privacy Rule;
- The incident consisted of inadvertent disclosure by a person authorized to access PHI at the Plan or its Business Associate to another person authorized to access PHI at the Plan or a Business Associate in the organized healthcare arrangement in which the Plan participates, and the PHI was not further used or disclosed in a manner disallowed under the Privacy Rule;
- The Plan has a good faith belief that the unauthorized person(s) to whom the disclosure was made would not reasonably have been able to retain the information; or
- The Plan has reasonably determined that the PHI’s access, use, or disclosure (taking into account the personal data elements involved, how the incident occurred, and who received the data) does not pose a significant risk of financial, reputational, or other harm to the affected individuals.

If one or more exceptions to the breach notice obligation applies under this Section 6.05(b), CSU will consider whether notice to some or all of the potentially affected individuals is nevertheless appropriate. If so, the Breach Contact (or his or her designee) will take steps to notify such individuals but will *not* be obligated to follow the specific timelines or steps outlined in Sections 6.05(c) through (e) below. Additionally, the Breach Contact (or his or her designee) will finish filling out the Breach Incident Log (see Form 10.09(b)) related to the incident.

If no exception applies, the Breach Contact will conduct, or direct others in the performance of, the procedures outlined in Sections 6.05(c) through (e) below.

In any case, CSU also will take into account any notice obligation that applies under relevant state privacy law, except to the extent that such state law is contrary to the HIPAA Breach Notice Rule; in that case, compliance with the Breach Notice Rule will prevail.

c. Preparing Breach Notices

If the Breach Notice Rule requires that CSU send notice to affected individuals, the Privacy Official (or his or her designee) will oversee the preparation of the notice, which will include determining whether receiving advice of counsel is necessary or prudent in the notice development.

Any notice drafted to satisfy the Breach Notice Rule will be written in plain language and will cover at least the following elements of information:

Breach Notice Content

Required Element	Example
Brief description of what happened, including the date of breach and (if known) the date of discovery)	<ul style="list-style-type: none"> ✓ on or around July 31, 2010, [entity's] Seattle offices experienced a break-in and theft of some office equipment, including several desktop computers ✓ the incident was discovered when staff returned for regular working hours on August 2, 2010 ✓ some of the missing desktops contained information necessary for administration of the [Name of Plan], in which you are enrolled as a [Name of Employer] employee
Types of PHI involved (e.g., name, SSN, DOB, home address, account numbers, diagnosis information)	<ul style="list-style-type: none"> ✓ types of information contained in the missing computers includes Plan enrollees' full names, Social Security numbers, and home addresses
Steps individuals should take to protect themselves from potential harm resulting from the breach	<ul style="list-style-type: none"> ✓ contact your financial institution to alert them to the possible theft of this personal information ✓ contact the free government ... <i>[free gov't service by website/address]</i> ✓ obtain credit monitoring services from a credit bureau to continually receive information about your credit status and observe specific activity in your name
Brief description of what CSU is doing to investigate the breach, mitigate harm to individuals, and protect against further incidents	<ul style="list-style-type: none"> ✓ immediately filed a police report with the appropriate authorities and cooperated in the police investigation of the theft ✓ actively monitoring the progress of the police investigation ✓ will make all reasonable efforts to recover the missing computers ✓ installed encryption protections on all portable devices that contain PHI
Contact procedures for individuals to ask questions, including a toll-free telephone number, e-mail address, website, or postal address	<ul style="list-style-type: none"> ✓ you may contact us at [URL address] or at 1-800-XXX-XXXX between 9:00 a.m. and 5:00 p.m. (Eastern Standard Time) with any questions about this letter ✓ you may visit the following website to learn of any new information about this incident, which will be updated at least weekly

d. Distributing Breach Notices

Individual HIPAA breach notices and, if applicable, media notices, will be sent without unreasonable delay and in no case later than 60 calendar days after discovery of the incident. *In addition to* taking the below steps, if the Plan determines during the investigation of the incident that possible misuse of the PHI may be imminent, the Plan may take more urgent action to contact the affected individuals, such as by telephone or other immediate medium.

In accordance with the Breach Notice Rule, CSU will take the following applicable steps to distribute the breach notice:

Individual Notice

- Notice will be sent by first-class mail to the individual's last-known address (or by e-mail if the affected individual agrees to electronic notice and the agreement hasn't been withdrawn);
- If the affected person is deceased, notice will be sent by first-class mail to the person's next-of-kin or personal representative, but only if CSU has their contact information;
- If the contact information for the affected individual is out of date, CSU will send a substitute form of notice reasonably calculated to reach the person, which could be by e-mail message, telephone, or other means (except that no substitute form of contact is necessary if the unreachable person is the next-of-kin or personal representative);
- If there are *ten or more* affected people who cannot be mailed the written notice due to insufficient or outdated contact information (taking into account the number whose notice was returned as undeliverable), CSU will either:
 - conspicuously post a hyperlink to the substitute notice on the Plan's website homepage for at least 90 days, *or*
 - provide the notice in major print or broadcast media where the affected individuals likely reside, *and*
 - the substitute notice will include a toll-free telephone number (active for at least 90 days) for individuals to contact the Plan to learn if their PHI was involved in the breach incident.

Media Notice

- If the breach incident affects the PHI of more than 500 residents of a State then, in addition to taking the individual notice steps above, CSU will direct a press release to prominent

media outlets serving that State (or smaller area where the affected people reside), which will cover the same topics required for the individual notice.

Additionally, the Breach Contact (or his or her designee) will finish filling out the Breach Incident Log (Form 10.09(b)) related to the incident.

e. Reporting Breach Incidents to HHS

The Breach Contact (or his or her designee) will notify HHS of each breach incident entered in the Plan's Breach Incident Log (Form 10.09(b)) for which no notice exception is available under the Breach Notice Rule. The report will be made by visiting the applicable HHS web site and filling out and electronically submitting the agency's breach report form. If a breach affects 500 or more individuals, the Plan will report to HHS at the same time that the Plan distributes the individual notices to affected people. If a breach affects fewer than 500 individuals, the Plan may notify HHS of such breaches on an annual basis, but no later than 60 days after the end of the calendar year in which the breach occurred.

f. Mitigation Steps for Breaches Originating from a Business Associate

All Business Associates must report to the Plan any breaches of PHI as soon as possible after discovery. The Plan will coordinate with each Business Associate to ensure that the above applicable steps are executed with respect to each breach incident. Such coordination may entail delegating to the applicable Business Associate the obligation to undertake relevant steps above on behalf of the Plan.

g. Documentation

CSU will maintain all Breach Incident Logs for a period of six (6) years.

h. Citations

45 CFR § 164.530(f)

45 CFR § 400 – 408

§ 13402 of HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009)

7.06 Document Retention

The Plan must retain copies of its Policies and Procedures and all communications that the HIPAA Privacy Rule requires to be in writing. The Plan must also retain records of actions or designations that the HIPAA Privacy Rule requires to be documented. Materials can be maintained in written or electronic form. They must be retained for at least six (6) years from the date of their creation or when they were last in effect (whichever is later).

Business Associates and Insurers will retain documents in their possession as required by the HIPAA Privacy Rule and Business Associate Agreements.

a. Document Retention Checklists

The following are checklists of materials that CSU will retain under this rule:

Documents	
<input type="checkbox"/> Privacy Policies and Procedures (this Manual)*	<input type="checkbox"/> Documentation that training has been provided to employees
<input type="checkbox"/> Authorizations*	<input type="checkbox"/> Information in Designated Record Set to which Participants and similar persons have access (see Section 6.02)
<input type="checkbox"/> Plan Amendments	
<input type="checkbox"/> Plan Amendment certifications	<input type="checkbox"/> Data Use Agreements (used in certain cases involving summary data disclosed for research, public health, or Health Care Operations purposes)
<input type="checkbox"/> Business Associate Agreements and Privacy Agreements for external EAPs*	
<input type="checkbox"/> Distribution of Privacy Notices*	
(*) Reflects materials to be maintained by Campus Privacy Contact.	

Key person identification	
<input type="checkbox"/> Name of Privacy Official	
<input type="checkbox"/> Names of Campus Privacy Contacts	

Other materials relating to particular actions by the Plan	
<input type="checkbox"/> Complaints about the HIPAA Privacy Rule or this Manual and their disposition, if any*	<input type="checkbox"/> Description of PHI disclosed *
<input type="checkbox"/> Documentation of sanctions applied to employees for not complying with the HIPAA Privacy Rule, if any*	<input type="checkbox"/> Copy of disclosure requests (or if made orally, statements describing the disclosures' purpose)*
<input type="checkbox"/> Notices that deny a person's access to PHI*	<input type="checkbox"/> Court orders, grand jury subpoenas, etc., where disclosure is required by law*
<input type="checkbox"/> Notices that delay a person's access to PHI*	<input type="checkbox"/> Written statements in connection with disclosures needed for other judicial/administrative processes, where the disclosure is not mandated by court order*
<input type="checkbox"/> Notices that explain whether the Plan will overturn a decision to deny a person access to PHI*	<input type="checkbox"/> Copies of written accountings*
<input type="checkbox"/> Notices that deny a person's request to amend PHI*	<input type="checkbox"/> Plan's notice terminating a restriction on uses or disclosures of PHI previously agreed to by the Plan*
<input type="checkbox"/> Notices that delay amendments to PHI*	<input type="checkbox"/> Person's agreement or request to terminate a restriction on uses or disclosures of PHI previously agreed to by the Plan*
<input type="checkbox"/> Statements of persons disagreeing with the Plan's decision to deny a request to amend PHI and any rebuttals of the statements*	<input type="checkbox"/> Other communications required by the Plan to be in writing, including requests for Confidential Communications.
<input type="checkbox"/> Disclosures of PHI for which a person is entitled to an accounting*	
<input type="checkbox"/> Written statements or other documentation in support of verifications made prior to disclosures*	
<input type="checkbox"/> Written statements by agencies or officials supporting suspension of an accounting of PHI disclosures (including oral statements documented by the Plan) *	
<input type="checkbox"/> Conclusion and supporting analysis from an expert that health information is de-identified	(*) Reflects materials to be maintained by Campus Privacy Contact.

b. Citations

45 CFR § 164.530(j)

8. Required Legal Documents

8.01 Overview

8.02 Privacy Notice

8.03 Authorization

8.01 Overview

The HIPAA Privacy Rule requires Covered Entities to use specific documents to accomplish certain tasks.

- A Privacy Notice describes the Plan's practices concerning its uses and disclosures of PHI and informs Participants of their rights and of the Plan's legal duties, with respect to PHI (see Section 8.02);
- A Participant's Authorization permits the Plan to use and disclose the Participant's PHI for purposes not otherwise permitted or required by the HIPAA Privacy Rule (see Section 8.03);
- An Amendment to the Plan document describes the Plan's permitted uses and disclosures of PHI (Systemwide Privacy Official responsible for Plan Amendment);
- A plan sponsor certification certifies that the Plan Sponsor has adopted the Plan Amendment and agrees to the restrictions on the uses and disclosures of PHI (Systemwide Privacy Official responsible for Plan Sponsor Certification); and
- A Privacy/Business Associate Agreement describes the permitted uses and disclosures of PHI by the Business Associate (Systemwide Privacy Official responsible for Plan Sponsor Certification); and

8.02 Privacy Notice

CSU will provide a Multi Benefit Plan Privacy Notice in Section 11.05 to satisfy the notice obligation for the HCRA and external EAP plans. Each Insurer or HMO will provide its own Privacy Notice to those Participants who receive insured Plan benefits, in accordance with the requirements of the HIPAA Privacy Rule. In addition, CSU will provide the Privacy Notice in Section 11.05 to new hires. In addition, CSU will provide a Multi Benefit Plan Privacy Notice to Participants upon request.

a. Identifying the Recipients

CSU will provide a Privacy Notice (see Section 11.05) to new enrollees under a self-funded Plan benefit at the time of enrollment. CSU will not provide a separate Privacy Notice to spouses or dependents, except for qualified beneficiaries who made independent COBRA elections (e.g., following a divorce or the death of an employee).

In addition, CSU will provide the Privacy Notice to all Business Associates and to workforce members who perform Plan functions, during their initial training and when necessary thereafter.

b. Distributing the Notice

CSU will provide the Privacy Notice by in-hand delivery or first-class mail.

CSU also may provide the Notice by e-mail, if the Participant has agreed to electronic notice and the agreement has not been withdrawn. CSU will provide a paper copy of the Notice if it knows that an e-mail transmission has failed.

CSU will prominently post the Notice on any web sites that it maintains that provide information about the Plan's services or benefits.

c. Revising the Notice

CSU will revise the Privacy Notice if its terms are affected by a change to the Plan's Policies and Procedures.

If the change is material (as determined by the Privacy Official), CSU will provide the revised Privacy Notice to Participants covered under a self-funded Plan benefit within sixty (60) days of the change. No material change will be implemented before the effective date of the revised

Privacy Notice (except where required by law). In addition, CSU will promptly provide revised Privacy Notices to Business Associates and workforce members who perform Plan functions.

d. Informing Participants of the Availability of the Notice

Once every three (3) years, CSU will inform all Participants of the Privacy Notice's availability and how to obtain a copy. The method used to send out this notification will be determined by the Privacy Official and the Campus Privacy Contacts.

e. Documenting Notices

All Privacy Notices will be documented and retained for a period of at least six (6) years from the date of creation or when last in effect, whichever is later.

f. Citations

45 CFR § 164.520(d)

8.03 Authorization

The HIPAA Privacy Rule requires the Plan to receive an Authorization from a Participant before using or disclosing PHI for purposes other than Treatment, Payment, Health Care Operations, or as otherwise permitted or required by the HIPAA Privacy Rule. The Plan may act on an Authorization only to the extent consistent with the terms of such Authorization. CSU must obtain the Participant's Authorization if CSU will be receiving any PHI, other than enrollment or HCRA claim appeals information from the health insurance carriers, HMOs, external EAP vendors or the HCRA claims administrator, unless such disclosure is required by law (see Section 5.06).

a. Providing the Authorization Form to Participants

CSU will provide an Authorization Form (see Section 11.06(f)) to Participant who requests that his or her PHI be disclosed to a third party (other than a personal representative).

CSU will provide each Participant with an Authorization Form if CSU wants to use or disclose the Plan's PHI for a purpose that requires Authorization (see Section 5.04).

b. Signing of the Authorization Form

The signing of an Authorization Form is voluntary. Participants may refuse to authorize use of their PHI.

c. Receiving the Signed Authorization Form

The Plan must have a signed Authorization Form from the Participant, before it can take an action that requires Authorization.

d. Determining the Validity of Authorization

Before the use or disclosure of PHI, the Plan will confirm that the Authorization is valid by verifying that:

- The expiration date or event triggering expiration has not passed;
- The Authorization was filled out completely;

- The Authorization has not been revoked; and
- The Authorization Form contains all the required elements.

e. Revocation of Authorization

At any time, the Participant may revoke the Authorization, provided that a revocation will not be effective if the Authorization was relied on as described in the Form. Requests for revocation of Authorizations must be submitted in writing to the Campus Privacy Contact (see Section 11.03). The Plan will not act upon an Authorization that has been revoked.

f. Documentation Requirement

All Authorizations and revocations of Authorizations will be documented and retained for a period of at least six (6) years from the date the Authorization is created or when it last was in effect, whichever is later.

g. Citations

45 CFR § 164.508

9. Guidelines for Policy and Procedure Changes

In order for the Policies and Procedures to remain current, CSU must consider modifying the Policies and Procedures to account for changed circumstances. Such changes may involve, for example, Amendments to the HIPAA Privacy Rule, adoption of a new group health plan, or termination of a Business Associate, among others.

The process for Policy and Procedure modification involves the following steps:

- Monitor changes that may impact the Policies and Procedures
- Assess the impact on the Policies and Procedures
- Modify the Policies and Procedures, if appropriate
- Distribute (and, if appropriate, provide training on) modified Policies and Procedures

The events for which a HIPAA impact assessment should be conducted include, but are not limited to, those described in the table beginning on the following page. The table also identifies the types of actions recommended to address the respective events. Each event will require specific review to determine an appropriate action plan.

The Privacy Official will generally be responsible for coordination of the Policies and Procedures under the HIPAA Privacy Rule. Accordingly, the recommended actions in the following table will typically be undertaken either directly by the Privacy Official or, at the direction of the Privacy Official, by others such as plan administrative staff, internal legal counsel, and/or external advisors.

(Note that references in the following table to various “Sections” are references to the respective Section of CSU’s HIPAA Privacy Manual.)

Event	Recommended Action(s)
<p><u><i>Change in CSU Operations:</i></u></p> <ul style="list-style-type: none"> • New staff members • New technology • New operating procedures 	<ul style="list-style-type: none"> • Monitor and update any changes in HIPAA Campus Privacy Contacts listed in Section 11.03. • Update and refer to Section 11.02 in the event of any change involving the Privacy Official. • Monitor changes in technology and business operating procedures involving processes for handling PHI under the Policies and Procedures. In particular, changes should be reviewed for any effect on Policies and Procedures in Sections 4 and 5. • Implement training appropriate to the level of any revisions in Policies and Procedures resulting from staffing, technology or operations changes. • Revise (and distribute revised) Notice of Privacy Practices, if applicable. (See Section 8.02(c) for additional information.)
<p><u><i>Rule Change:</i></u> Changes in the HIPAA Privacy Rule or related rules (for example, the final Security Rule taking effect). Changes may occur in statutes, regulations, agency guidance, or case law.</p>	<ul style="list-style-type: none"> • Monitor developments changing the applicable rules. • Identify specific Policies and Procedures affected by the development. • Assess need for modifications to the Policies and Procedures. • Revise Policies and Procedures – including legal documents referenced in Section 8 and Participant forms referenced in Section 6 – as appropriate. • Distribute revised Policies and Procedures and training materials. • If applicable, distribute revised HIPAA Privacy Notice and Sponsor Certification. • If applicable, negotiate modifications to Business Associate agreements and other vendor contracts.
<p><u><i>Business Associate Addition:</i></u> Adding a new Business Associate. Change may occur at renewal, mid-term (for example, replacement of prior vendor), or by reason of a merger or other transaction affecting an existing Business Associate.</p>	<ul style="list-style-type: none"> • Monitor circumstances leading to addition of Business Associate. If possible, include model Business Associate agreement in any applicable RFP specifications. • Negotiate and customize the Business Associate agreement and present it for execution to the vendor. • Amend Section 11.04(b) (“Log of Business Associate Agreements”) and any other documents referring to the Business Associate. • If change coincides with a change in any Plan, refer to guidelines below on “Termination of Group Health Plan” or “Addition or Name Change in Group Health Plan” as applicable.

Event	Recommended Action(s)
<p><u>Business Associate Termination:</u> Terminating an existing Business Associate. Change may occur at renewal, mid-term (for example, a termination for performance failure), or by reason of a merger or other transaction affecting the Business Associate.</p>	<ul style="list-style-type: none"> • Monitor circumstances requiring termination of Business Associate. • Clarify Plan’s needs and, if necessary, negotiate termination provisions with the Business Associate concerning issues such as transfer of data, and continued HIPAA contact responsibilities delegated to the Business Associate. In particular, will vendor retain any PHI? If so, who are the contacts for continued access to PHI? Consider agents and subcontractors of Business Associate. • Amend Section 11.04(b) (“Log of Business Associate Agreements”) and any other documents referring to the Business Associate. • If change coincides with a change in any Plan, refer to guidelines below on “Termination of Group Health Plan” or “Addition or Name Change in Group Health Plan” as applicable.
<p><u>Insurer Addition:</u> Adding a health plan insurer.</p>	<ul style="list-style-type: none"> • Monitor circumstances leading to addition of an insurer. • Obtain and preserve contact information for purposes of referring future PHI requests. • Review and modify any references to the insurer in the Policies and Procedures (for example, references in Section 11.05 and the Notice of Privacy Practices), as appropriate. • Furnish Plan Sponsor Certification, as appropriate (if PHI will be obtained from the insurer). • Obtain copy of insurer’s Notice of Privacy Practices if making it available on request to Participants.
<p><u>Insurer Termination or Policy Revision:</u> Terminating a health plan insurer, or accepting a revised group insurance policy or contract by existing insurer.</p>	<ul style="list-style-type: none"> • Monitor circumstances requiring termination of the insurer or acceptance of a revised group insurance policy or contract. • Update and preserve contact information for purposes of referring requests for PHI maintained by insurer under a prior policy or contract. • Review and modify any references to the insurer in the Policies and Procedures (for example, references in Section 11.05 and the Notice of Privacy Practices), as appropriate. (Retain listing but mark as “former” carrier, if appropriate.)

Event	Recommended Action(s)
<p><u><i>Addition or Name Change in Group Health Plan:</i></u> Adding a health plan, or changing the current Plan name.</p>	<ul style="list-style-type: none"> • Monitor addition of a health plan potentially subject to the HIPAA Privacy Rule (or of a change in the name of an existing Plan). • Determine if new plan is subject to the HIPAA Privacy Rule, and whether it is a separate group health plan or a component of an existing Plan. • Determine application of “organized health care arrangement” to all Plans, including modifications to Policies and Procedures and use of joint Notice of Privacy Practices. • Amend Section 11.01 (“Covered Plans”) and any other documents or forms referring to the Plans, as appropriate. • Refer to guidelines above on “Business Associate Addition” or “Insurer Addition”, as applicable. • Consider if changes in personnel are also implicated.
<p><u><i>Termination in Group Health Plan:</i></u> Terminating a Plan or a component Plan subject to the HIPAA Privacy Rule.</p>	<ul style="list-style-type: none"> • Monitor circumstances leading to deletion of a Plan subject to the HIPAA Privacy Rule. • Determine impact on application of “organized health care arrangement” to all Plans, including modifications to Policies and Procedures and use of joint Notice of Privacy Practices. • Amend Section 11.01 (“Covered Plans”) and any other documents or forms referring to the Plans, as appropriate. • Refer to guidelines above on “Business Associate Termination” or “Insurer Termination or Policy Revision” as applicable. • Consider if changes in personnel also implicated. • Identify and preserve contact information for PHI maintained in connection with the terminated Plan.

10. HIPAA Resources

The [complete suite](#) of HIPAA Administrative Simplification Regulations can be found at 45 CFR Parts [160](#), [162](#), and [164](#), and includes:

- Transactions and Code Set Standards
- Identifier Standards
- Privacy Rule
- Security Rule
- Enforcement Rule

[HITECH Act \(Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009\)](#)

[Interim Final Regulation Text: Breach Notification for Unsecured Protected Health Information](#)

[Proposed Regulation Text: Genetic Information Nondiscrimination Act \[Impact on\] Standards for Privacy of Individually Identifiable Health Information](#)

[The Department of Health and Human Services Office of Civil Rights HIPAA privacy website](#)

11. Key Resources and Forms

11.01 Covered Plans

11.02 Privacy Official

11.03 Other Contacts

11.04 Insurers

11.05 Notice of Privacy Practices

11.06 Participant Forms

11.07 Breach Report Forms

11.01 Covered Plans

CSU sponsors the following group health plan(s):

- CalPERS Health Care Providers (medical and prescription drug coverage)
- Delta Dental (dental coverage)
- PMI Delta Care DMO (dental coverage)
- Vision Service Plan (VSP) (vision)
- Health Care Reimbursement Account (HCRA) Plan
- External EAPs that provide counseling services

11.02 Privacy Official

a. Privacy Official Designation

The following person is designated as the Privacy Official:

Name: Michelle Hamilton

Title: Manager, Benefits and HR Programs

Address: California State University, Office of the Chancellor
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4210

Phone: (562) 951-4413

Fax: (562) 951-4954

Email: mhamilton@calstate.edu

b. Sample Privacy Official Job Description

The Privacy Official shall be responsible for coordinating employer's policies and procedures under HIPAA's privacy rules, as revised from time-to-time, monitoring compliance with those rules, and making decisions with respect to any issues that arise under such rules. The Privacy Official shall report to the Assistant Vice Chancellor, Human Resources Management.

c. Essential Duties - General

- *Serve as the leader of CSU's HIPAA privacy workgroup and focal point for privacy compliance-related activities*
- *With the assistance of other CSU staff, implement HIPAA privacy policies and procedures for CSU's group health plan arrangement*
- *Assist in the interpretation of the state and federal privacy rules and act as the designated decision-maker for issues and questions, in coordination with legal counsel*
- *Oversee training of Campus Privacy Contacts*
- *May serve as internal and external liaison and resource between the CSU group health plan and other entities (employer's officers, vendors, Office of Civil Rights, other legal entities) for purposes of any compliance reviews or investigations and to ensure that CSU's privacy practices are implemented, consistent, and coordinated or may delegate this responsibility to the Campus Privacy Contacts*
- *Periodically revise the HIPAA privacy Policies and Procedures in light of changes to the rules, or changes in group health plan practices or in the flow of PHI*

d. Essential Duties – Specific

- *Along with the assistance of the Campus Privacy Contacts, develop procedures to inventory and document the uses and disclosures of protected health information (PHI)*
- *Develop and implement overall privacy policies and procedures as applicable for the employer group health plan arrangement*

- *Develop and implement appropriate firewalls between CSU functions and the functions of the group health plan arrangement*
- *Draft and have the Campus Privacy Contacts distribute the HIPAA privacy notice*
- *Serve or appoint the Campus Privacy Contacts as the designated contact person in the privacy notice and receive questions and complaints related to the protection of PHI, participant privacy, and violations of CSU's privacy policies and procedures*
- *Have the Campus Privacy Contacts establish mechanisms and monitor processes to ensure participants' rights to restrict, amend, have access to, and receive an accounting of their health information*
- *Have the Campus Privacy Contacts establish and administer a process to receive, document, track, investigate, and take action (including developing sanctions) on all complaints regarding CSU's privacy policies and procedures*
- *Ensure that CSU develops and maintains appropriate privacy authorization forms*
- *Ensure that amendments to plan documents are addressed*
- *Along with the assistance of the Campus Privacy Contacts, ensure that all documentation required by the privacy rule is maintained and retained for at least six (6) years from the date it was created or was last in effect, whichever is later*
- *Along with the assistance of the Campus Privacy Contacts, oversee and ensure delivery of privacy training and orientation to staff*
- *Monitor changes to the HIPAA privacy and security rules, including federal and state laws and regulations*
- *The Privacy Official shall have the sole authority and discretion to delegate the above tasks or portions thereof to other individuals within CSU (such as the Campus Privacy Contacts) or to consultants, contractors or other specialists, as appropriate, provided that the Privacy Official monitors such activities in good faith for purposes of achieving compliance with HIPAA.*

11.03 Other Contacts

Each campus and the Chancellor's Office will have a "Campus Privacy Contact" responsible for responding to Participants exercising their rights described in Section 6 and for other duties specified below. The Benefits Representative at each campus and the Chancellor's Office shall be the Campus Privacy Contact for each campus.

The Campus Privacy Contacts will be responsible for the following duties:

- Ensure privacy training and orientation of appropriate campus staff
- Ensure that CSU's privacy Policies and Procedures are implemented, consistent and coordinated and serve as internal and external liaison and resource between the employer group health plans and other entities for privacy purposes (e.g., compliance reviews, etc.)
- Developing a procedure to inventory and document the uses and disclosures of protected health information
- Distribution of HIPAA privacy notices
- Be the designated contact person to receive participant requests regarding their protected health information, complaints and questions regarding CSU's privacy policies and procedures
- Forward all such requests immediately to the Privacy Official, unless it is appropriate to direct the Participant making the request to a health insurance carrier or HMO.
- Ensure that all documentation required by the privacy rule is maintained and retained for at least six (6) years from the date it was created or was last in effect, whichever is later.

11.04 Insurers

The following is a list of the Plan(s) Insurers as of February 17, 2010. The Privacy Official will maintain an updated list of the Plan(s) Insurers.

Insurer	Policy identifying information
CalPERS Health Care Providers	Medical / Rx
Delta Dental	Dental
PMI Delta Care DMO	Dental
Vision Service Plan	Vision

11.05 Notice of Privacy Practices

Instructions for Privacy Notice

The Privacy Notice included in Section 11.05 is for distribution to participants in the HCRA plan and external EAPs.

Note that if a use or disclosure is prohibited or materially limited by another law — e.g., a more stringent state law — the notice must reflect the more stringent requirements (45 CFR 164.520(b)(1)(ii)).

The notice must describe how the individual may exercise each individual right and should indicate where to submit requests.

Notice of Privacy Practices

CSU Privacy Notice

Please carefully review this notice. It describes how medical information about you may be used and disclosed and how you can get access to this information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes numerous requirements on the use and disclosure of individual health information by employer health plans. This information, known as protected health information, includes almost all individually identifiable health information held by a plan – whether received in writing, in an electronic medium, or as an oral communication. This notice describes the privacy practices of the following group health plans: health care reimbursement account and employee assistance plans. The plans covered by this notice may share health information with each other if necessary, to carry out treatment, payment, or health care operations. These plans are collectively referred to as the Plan in this notice, unless specified otherwise.

The Plan's duties with respect to health information about you

The Plan is required by law to maintain the privacy of your health information and to provide you with this notice of the Plan's legal duties and privacy practices with respect to your health information. If you participate in an insured plan option, you will receive a notice directly from the Insurer. It's important to note that these rules apply to the Plan, not California State University as an employer – that's the way the HIPAA rules work. Different policies may apply to other California State University programs or to data unrelated to the Plan.

How the Plan may use or disclose your health information

The privacy rules generally allow the use and disclosure of your health information without your permission (known as an authorization) for purposes of health care treatment, payment activities, and health care operations. Here are some examples of what that might entail:

Treatment includes providing, coordinating, or managing health care by one or more health care providers or doctors. Treatment can also include coordination or management of care between a provider and a third party, and consultation and referrals between providers. *For example, the Plan may share your health information with physicians who are treating you.*

Payment includes activities by this Plan, other plans, or providers to obtain premiums, make coverage determinations, and provide reimbursement for health care. This can include eligibility determinations, reviewing services for medical necessity or appropriateness, utilization management activities, claims management, and billing; as well as “behind the scenes” plan functions such as risk adjustment, collection, or reinsurance. *For example, the Plan may share information about your coverage or the expenses you have incurred with another health plan in order to coordinate payment of benefits.*

Health care operations include activities by this Plan (and in limited circumstances other plans or providers) such as wellness and risk assessment programs, quality assessment and improvement activities, customer service, and internal grievance resolution. Health care operations also include vendor evaluations, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, and business planning and development. *For example, the Plan may use information about your claims to audit the third parties that approve payment for Plan benefits.*

The amount of health information used, disclosed or requested will be limited and, when needed, restricted to the minimum necessary to accomplish the intended purposes, as defined under the HIPAA rules. If the Plan uses or discloses PHI for underwriting purposes, the Plan will not use or disclose PHI that is your genetic information for such purposes. The Plan may contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you, as permitted by law.

How the Plan may share your health information with California State University

The Plan, or its health insurer or HMO, may disclose your health information without your written authorization to California State University for plan administration purposes. California State University *agrees* not to use or disclose your health information other than as permitted or required by the Plan documents and by law. Chancellor's Office HR staff and campus HR and benefit officers are the only California State University employees who will have access to your health information for plan administration functions.

Here's how additional information may be shared between the Plan and California State University, as allowed under the HIPAA rules:

- The Plan, or its insurer or HMO, may disclose "summary health information" to California State University if requested, for purposes of obtaining premium bids to provide coverage under the Plan, or for modifying, amending, or terminating the Plan. Summary health information is information that summarizes participants' claims information, from which names and other identifying information have been removed.
- The Plan, or its insurer or HMO, may disclose to California State University information on whether an individual is participating in the Plan or has enrolled or disenrolled in an insurance option or HMO offered by the Plan.

In addition, you should know that California State University cannot and will not use health information obtained from the Plan for any employment-related actions. However, health information collected by California State University from other sources, for example under the Family and Medical Leave Act, Americans with Disabilities Act, or workers' compensation is *not* protected under HIPAA (although this type of information may be protected under other federal or state laws).

Other allowable uses or disclosures of your health information

In certain cases, your health information can be disclosed without authorization to a family member, close friend, or other person you identify who is involved in your care or payment for your care. Information about your location, general condition, or death may be provided to a similar person (or to a public or private entity authorized to assist in disaster relief efforts). You'll generally be given the chance to agree or object to these disclosures (although exceptions may be made – for example, if you're not present or if you're incapacitated). In addition, your health information may be disclosed without authorization to your legal representative.

The Plan also is allowed to use or disclose your health information without your written authorization for the following activities:

Workers' compensation	Disclosures to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with the laws
Necessary to prevent serious threat to health or safety	Disclosures made in the good-faith belief that releasing your health information is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety, if made to someone reasonably able to prevent or lessen the threat (or to the target of the threat); includes disclosures to help law enforcement officials identify or apprehend an individual who has admitted participation in a violent crime that the Plan reasonably believes may have caused

	serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody
Public health activities	Disclosures authorized by law to persons who may be at risk of contracting or spreading a disease or condition; disclosures to public health authorities to prevent or control disease or report child abuse or neglect; and disclosures to the Food and Drug Administration to collect or report adverse events or product defects
Victims of abuse, neglect, or domestic violence	Disclosures to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or domestic violence, as required by law or if you agree or the Plan believes that disclosure is necessary to prevent serious harm to you or potential victims (you'll be notified of the Plan's disclosure if informing you won't put you at further risk)
Judicial and administrative proceedings	Disclosures in response to a court or administrative order, subpoena, discovery request, or other lawful process (the Plan may be required to notify you of the request or receive satisfactory assurance from the party seeking your health information that efforts were made to notify you or to obtain a qualified protective order concerning the information)
Law enforcement purposes	Disclosures to law enforcement officials required by law or legal process, or to identify a suspect, fugitive, witness, or missing person; disclosures about a crime victim if you agree or if disclosure is necessary for immediate law enforcement activity; disclosure about a death that may have resulted from criminal conduct; and disclosure to provide evidence of criminal conduct on the Plan's premises
Decedents	Disclosures to a coroner or medical examiner to identify the deceased or determine cause of death; and to funeral directors to carry out their duties
Organ, eye, or tissue donation	Disclosures to organ procurement organizations or other entities to facilitate organ, eye, or tissue donation and transplantation after death
Research purposes	Disclosures subject to approval by institutional or private privacy review boards, subject to certain assurances and representations by researchers about the necessity of using your health information and the treatment of the information during a research project
Health oversight activities	Disclosures to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, and compliance with regulatory programs or civil rights laws
Specialized government functions	Disclosures about individuals who are Armed Forces personnel or foreign military personnel under appropriate military command; disclosures to authorized federal officials for national security or intelligence activities; and disclosures to correctional facilities or custodial law enforcement officials about inmates
HHS investigations	Disclosures of your health information to the Department of Health and Human Services to investigate or determine the Plan's compliance with the HIPAA privacy rule

Except as described in this notice, other uses and disclosures will be made only with your written authorization. You may revoke your authorization as allowed under the HIPAA rules. However, you can't revoke your authorization with respect to disclosures the Plan has already made. You will be notified of any unauthorized access, use or disclosure of your unsecured health information as required by law.

Your individual rights

You have the following rights with respect to your health information the Plan maintains. These rights are subject to certain limitations, as discussed below. This section of the notice describes how you may exercise each individual right. See the table at the end of this notice for information on how to submit requests.

a. Right to request restrictions on certain uses and disclosures of your health information and the Plan's right to refuse

You have the right to ask the Plan to restrict the use and disclosure of your health information for treatment, payment, or health care operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death – or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.

The Plan is not required to agree to a requested restriction. If the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose health information about you if you need emergency treatment, even if the Plan has agreed to a restriction.

Effective February 17, 2010, an entity covered by these HIPAA rules (such as your health care provider) or its business associate must comply with your request that health information regarding a specific health care item or service not be disclosed to the Plan for purposes of payment or health care operations if you have paid for the item or service, in full out of pocket.

b. Right to receive confidential communications of your health information

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations.

If you want to exercise this right, your request to the Plan must be in writing and you must include a statement that disclosure of all or part of the information could endanger you.

c. Right to inspect and copy your health information

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "designated record set." This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. The Plan may deny your right to access, although in certain circumstances you may request a review of the denial. If you want to exercise this right, your request to the Plan must be in writing. Within 30 days of receipt of your request (60 days if the health information is not accessible onsite), the Plan will provide you with:

- the access or copies you requested;
- a written denial that explains why your request was denied and any rights you may have to have the denial reviewed or file a complaint; or
- a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

The Plan may provide you with a summary or explanation of the information instead of access to or copies of your health information, if you agree in advance and pay any applicable fees. The Plan also may charge reasonable fees for copies or postage.

If the Plan doesn't maintain the health information but knows where it is maintained, you will be informed of where to direct your request.

Effective February 17, 2010, you may request an electronic copy of your health information if it is maintained in an electronic health record. You may also request that such electronic health information be sent to another entity or person, so long as that request is clear, conspicuous and specific. Any charge that is assessed to you for these copies, if any, must be reasonable and based on the Plan's cost.

d. Right to amend your health information that is inaccurate or incomplete

With certain exceptions, you have a right to request that the Plan amend your health information in a designated record set. The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete, was not created by the Plan (unless the person or entity that created the information is no longer available), is not part of the designated record set, or is not available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal, or administrative proceedings). If you want to exercise this right, your request to the Plan must be in writing, and you must include a statement to support the requested amendment. Within 60 days of receipt of your request, the Plan will:

- make the amendment as requested;
- provide a written denial that explains why your request was denied and any rights you may have to disagree or file a complaint; or
- provide a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

e. Right to receive an accounting of disclosures of your health information

You have the right to a list of certain disclosures of your health information the Plan has made. This is often referred to as an "accounting of disclosures." You generally may receive this accounting if the disclosure is required by law, in connection with public health activities, or in similar situations listed in the table earlier in this notice, unless otherwise indicated below.

You may receive information on disclosures of your health information for up to six years before the date of your request. You do not have a right to receive an accounting of any disclosures made:

- for treatment, payment, or health care operations;
- to you about your own health information;
- incidental to other permitted or required disclosures;
- where authorization was provided;
- to family members or friends involved in your care (where disclosure is permitted without authorization);
- for national security or intelligence purposes or to correctional institutions or law enforcement officials in certain circumstances; or
- as part of a "limited data set" (health information that excludes certain identifying information).

In addition, your right to an accounting of disclosures to a health oversight agency or law enforcement official may be suspended at the request of the agency or official.

If you want to exercise this right, your request to the Plan must be in writing. Within 60 days of the request, the Plan will provide you with the list of disclosures or a written statement that the time period for providing this list will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request. You may make one request in any 12-month period at no cost to you, but the Plan may charge a fee for subsequent requests. You'll be notified of the fee in advance and have the opportunity to change or revoke your request.

f. Right to obtain a paper copy of this notice from the Plan upon request

You have the right to obtain a paper copy of this privacy notice upon request.

Changes to the information in this notice

The Plan must abide by the terms of the privacy notice currently in effect. This notice takes effect on February 17, 2010. However, the Plan reserves the right to change the terms of its privacy policies, as described in this notice, at any time and to make new provisions effective for all health information that the Plan maintains. This includes health information that was previously created or received, not just health information created or received after the policy is changed. If changes are made to the Plan's privacy policies described in this notice, you will be provided with a revised privacy notice mailed to your home address on file.

Complaints

If you believe your privacy rights have been violated or your Plan has not followed its legal obligations under HIPAA, you may complain to the Plan and to the Secretary of Health and Human Services. You won't be retaliated against for filing a complaint. For complaints regarding the Employee Assistance Program (EAP), contact the campus benefits officer. For complaints regarding the Health Care Reimbursement Account Plan, contact CSU Systemwide Human Resources Management (HRM) at CSU Office of the Chancellor – Attention Human Resources Management, 401 Golden Shore, Long Beach, CA 90802. Complaints should be filed in writing and such written document should include a description of the nature of the particular complaint.

Contact

For more information on the Plan's privacy policies or your rights under HIPAA, contact the campus benefits office.

11.06 Participant Forms

The following forms are included in this section:

- 11.06(a) Request for Access to Inspect and Copy
- 11.06(b) Request to Amend
- 11.06(c) Request for Restricted Use
- 11.06(d) Request for Confidential Communications
- 11.06(e) Request for Accounting of Non-Routine Disclosures
- 11.06(f) Authorization to Use and/or Disclosure

a. Request for Access to Inspect and Copy**Instructions for Responding to a Request for Access to Inspect and Copy****Directions for CSU:**

Providing Form. If any person wishes to request access to inspect and copy Personal health plan information for the HCRA and external EAP Plans, the Campus Privacy Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form, the Campus Privacy Contact should initial and date top right corner and must verify that Part I (Request for Access to Inspect and Copy Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in sections A and B must be marked, and the form must be signed and dated. If the person requesting Personal health plan information is not the subject of the information, the Campus Privacy Contact should verify the identity and authority of the person and follow the procedures detailed in Section 4.03.

If Part I is incomplete, the Campus Privacy Contact should return it to the person for completion. Once Part I of the Form is complete, the Campus Privacy Contact should forward it to the Privacy Official.

Determination of Request. Upon receipt of this Form with Part I properly completed, the Privacy Official will respond by completing Part II (Determination of Request for Access to Inspect and Copy Personal Health Plan Information, within the timeframes detailed in [Section 6.02](#).

Note that although a Designated Record Set includes the Plan's enrollment and Payment information, it does not include CSU's enrollment and Payment records.

Part I - Request for Access to Inspect and Copy Personal Health Plan Information

Form Received By

Date

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "Designated Record Set" maintained by the HCRA plan or other group health plans sponsored by the California State University (collectively, the "Plan"). This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. In addition, the Plan may deny your right to access, although in certain circumstances you may request a review of the denial. You may also request an electronic copy of your health information if it is maintained in an "Electronic Health Record," or request that such electronic health information be sent to another entity or person, so long as that request is clear, conspicuous and specific.

The Plan may provide you with a summary or explanation of the information in your health plan records instead of access to or copies of your records, if you agree in advance and pay any applicable fees. The Plan may also charge reasonable fees for copies or postage.

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Records You Are Requesting	2a. Relationship to Employee Self <input type="checkbox"/> Spouse <input type="checkbox"/> Child <input type="checkbox"/> Other <input type="checkbox"/>
3. Your Name	3a. Your Relationship to Person in Box 2 Self <input type="checkbox"/> Spouse <input type="checkbox"/> Parent <input type="checkbox"/> Child <input type="checkbox"/> <input type="checkbox"/> Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

Section A: Requested Personal Records.

Please identify the personal health plan information in your health plan records you are requesting access to, including the time period to which the information relates:

Section B: Methods of Access.

I wish to inspect and copy the personal health plan information described in Section A using the following method(s):

- ☐ I wish to inspect the records requested in Section A in person. I will arrange a mutually agreeable time to come to the Plan by contacting the Campus Privacy Contact.
- ☐ I wish to copy the records requested in Section A in person. I will arrange a mutually agreeable time to come to the Plan by contacting the Campus Privacy Contact. I understand that I will be charged and I agree to pay the cost of copying at ____ per page.
- ☐ I wish to have copies of the records requested in Section A sent directly to me, at the address in Box 4. I understand that I will be charged and I agree to pay the cost of copying at ____ per page plus postage.
- ☐ I wish to have electronic copies of the records requested in Section A that are a part of an Electronic Health Record sent directly to me, at the address in Box 4. I understand that I will be charged and I agree to pay the associated cost.
- ☐ I wish to have electronic copies of the records requested in Section A that are a part of an Electronic Health Record sent to the following person or entity: _____, at the address in Box 4. I understand that I will be charged and I agree to pay the associated cost.
- ☐ I wish to have the information requested in Section A summarized (instead of receiving the entire record) and sent to me at the address in Box 4. I understand that I will be charged for the summary provided and I agree to pay the cost of preparing the summary, any copying at ____ per page, and postage.

Please return completed form to: **Campus Privacy Contact**

[Insert title]

[Insert address]

[Insert phone number]

Signature

Date

Part II - Determination of Request for Access to Inspect and Copy Personal Health Plan Records

Form Part II Prepared By _____

Date Part II
Issued _____

After reviewing your request for access to inspect and/or copy personal health plan records, the Privacy Official has made the following determination **[check one (1)]**:

- ☐ **Request granted** (see Section A below).
- ☐ **Request partially granted and partially denied** (see Section A and B or C below).
- ☐ **Request denied with no right to review** (see Section B below).
- ☐ **Request denied with right to review** (see Section C below).

Section A: Request Granted

Your request for access to inspect and/or copy personal health plan records is granted **[in full / in part]**. **[All / Some]** of the health information you requested is available to you for inspection or copying, or both. If you requested to review the records in person, please contact the Privacy Official at _____ [insert phone number] to coordinate this request. If you requested that the records or a summary be sent to you, a copy is attached.

Section B: Request Denied with No Right to Review

Your request for access to inspect and copy personal health plan records is denied **[in full / in part]** for the following reasons **[check all that apply]**:

- ☐ The information requested is psychotherapy notes.
- ☐ The information is for civil, criminal, or administrative proceedings.
- ☐ The information is created for research and you agreed to forgo access while the research is in progress.
- ☐ The information is subject to the Privacy Act, 5 U.S.C. 522(a) and access may be denied under that law.
- ☐ The information was obtained from someone other than a health care provider under a promise of confidentiality and access would reveal the source.
- ☐ The information requested is not maintained by the Plan. The Campus Privacy Contact does not know who maintains the specific information requested.
- ☐ The information requested is not maintained by the Plan. The information is maintained by _____. Please contact them for access to the information.

Section C: Request Denied with Right to Review

Your request for access to inspect and/or copy personal health plan records has been denied **[in full / in part]** because a licensed health care professional has determined that the access is reasonably likely to endanger an individual. You have a right to ask the Plan to have the denial reviewed by another licensed health care professional.

If you wish to ask the Plan to review this denial, please send a written request to the Privacy Official, _____ [insert title] at _____ [insert address]. For more information, please contact the Privacy Official at _____ [insert phone number].

If you have been denied access to inspect and copy PHI, you may complain to the Plan or to the Secretary of the U.S. Department of Health and Human Services at <http://www.hhs.gov/ocr/privacy/howtofile.htm> For more information, please contact the Privacy Official at the above address and phone number.

Name of Plan Representative

Signature of Plan Representative

Date of Determination

b. Request to Amend Personal Health Plan Information

Instructions for Responding to a Request for Access to Inspect and Copy

Directions for CSU:

Providing Form. If any person wishes to request that the HCRA Plan or an external EAP amend his or her personal health plan information, the Campus Privacy Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form, the Campus Privacy Contact must verify that Part I (Request to Amend Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the Form must be signed and dated. If the person requesting personal health plan information is not the subject of the information, the Campus Privacy Contact should verify the identity and authority of the person and follow the procedures detailed in Section 4.03.

If Part I of the Form is incomplete, the Campus Privacy Contact should return it to the person for completion. Once Part I of the Form is complete, the Campus Privacy Contact should forward it to the Privacy Contact.

Determination of Request. Upon receipt of this Form with Part I properly completed, the Privacy Official will respond by completing Part II (Determination of Request to Amend Personal Health Plan Information), within the timeframes detailed in Section 6.03.

Part I - Request to Amend Personal Health Plan Information

Form Received By

Date

With certain exceptions, you have a right to request that the HCRA plan or other group health plans sponsored by the California State University (collectively, the "Plan") amend your health information in a "Designated Record Set." The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete; was not created by the Plan (unless the person or entity that created the information is no longer available); is not part of the Designated Record Set; or would not be available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal or administrative proceedings).

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Records You Are Requesting	2a. Relationship to Employee Self <input type="checkbox"/> Spouse <input type="checkbox"/> Child <input type="checkbox"/> Other <input type="checkbox"/>
3. Your Name	3a. Your Relationship to Person in Box 2 Self <input type="checkbox"/> Spouse <input type="checkbox"/> Parent <input type="checkbox"/> Child <input type="checkbox"/> <input type="checkbox"/> Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

I request that the Plan amend the following information in a personal health plan record [describe the information that is the subject of the Amendment request]:

The identified information should be amended because:

I understand that if the Plan approves my request to amend a health plan record, the Plan will not necessarily delete the original information in the Designated Record Set, but instead may choose to identify the information in the Designated Record Set(s) that is the subject of my request for Amendment and provide a link to the location of the Amendment

Signature

Date

Part II - Determination of Request to Amend Personal Health Plan Information

Form Part II Prepared
By

Date Part II Issued

☐ Request Approved

☐ Request Denied for the following reasons [check all that apply]:

- ☐ The PHI or record was not created by the Plan.
- ☐ The PHI or record is not part of one of the Plan's Designated Record Sets.
- ☐ The PHI or record is not available for inspection under the HIPAA Privacy Rule.
- ☐ The PHI or record is accurate and complete referring.

If your request has been denied, you have the right to submit a statement of disagreement and the basis for such disagreement (limited to five (5) pages) to the Privacy Official at _____ [insert address]. In response, the Privacy Official will send you a copy of any rebuttal statement that is prepared. If you submit a statement of disagreement, when the Plan makes future disclosures of your disputed PHI or record, a copy of your request, the denial, and any disagreement and rebuttal will be attached to the disclosed PHI or record.

If your request has been denied and you choose not to submit a statement of disagreement, you may still ask the Plan to include a copy of your Amendment and the denial along with any future disclosures of the health information that is the subject of the Amendment request.

If you have been denied access to inspect and copy PHI, you may complain to the Plan or to the Secretary of the U.S. Department of Health and Human Services at <http://www.hhs.gov/ocr/privacyhowtofile.htm>. For more information, please contact the Privacy Official at _____ [insert phone number].

Name of Plan Representative

Signature of Plan Representative

Date of Determination

c. Restricted Access

Instructions for Responding to a Request for Restricted Use of PHI

Directions for CSU:

Providing Form. If any person wishes to request that the Plan (for any plan coverage) restrict or terminate a restriction on the Plan's use and disclosure of his or her PHI, the Campus Privacy Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form, the Campus Privacy Contact must verify that Part I (Request for Restricted Use Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting the restricted use of PHI is not the subject of the PHI, the Campus Privacy Contact should verify the identity and authority of the person and follow the procedures detailed in Section 4.03.

If Part I of the Form is incomplete, the Campus Privacy Contact should return it to the person for completion. Once Part I of the Form is complete, the Campus Privacy Contact should forward it to the Privacy Official.

Determination of Request for Restricted Use of PHI. When Part I, Section A has been completed, the Privacy Official will respond by completing Part II (Determination of Request for Restricted Use of Personal Health Plan Information), within the timeframes detailed in Section 6.04. Note that no restrictions will be approved (see Section 6.04).

Part I - Request for Restricted Use of Personal Health Plan Information

Form Received By _____

Date _____

You have the right to ask the Plan to restrict the use and disclosure of your health information for Treatment, Payment, or Health Care Operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or Payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death — or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.

The Plan is not required to agree to a requested restriction. If the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose health information about you if you need emergency Treatment, even if the Plan has agreed to a restriction.

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Records You Are Requesting	2a. Relationship to Employee Self <input type="checkbox"/> Spouse <input type="checkbox"/> Child <input type="checkbox"/> Other <input type="checkbox"/>
3. Your Name	3a. Your Relationship to Person in Box 2 Self <input type="checkbox"/> Spouse <input type="checkbox"/> Parent <input type="checkbox"/> Child <input type="checkbox"/> <input type="checkbox"/> Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

Section A: Request to Restrict Use and Disclosure of Personal Health Plan Information

I request that the use and disclosure of personal health plan information for the person in Box 2 be restricted in the manner described below:

☐ I have / ☐ I have not: already paid the health care provider in full for the items or services related to this information.

I understand that the Plan may deny this request. I also understand that the Plan may remove this restriction in the future if I am notified in advance.

Section B: Request to Terminate Restricted Use and Disclosure of Personal Health Plan Information

☐ I request that the restriction on the use and disclosure of personal health plan information made on _____ [Date Initial Request Made] be terminated. I understand that upon receipt of this form, the Plan will terminate the previously accepted restriction. Once a restriction has been terminated, the Plan will use and disclose personal health plan information as permitted or required by law.

☐ I agreed orally to terminate the restricted use and disclosure of personal health plan information belonging to the person in Box 2 made on _____ [Date Initial Request Made]. This serves as formal documentation of that oral agreement.

Signature _____

Date _____

Part II - Determination of Request for Restricted Use of Personal Health Plan Information

Form Part II Prepared By

Date Part II
Issued

After reviewing your request to restrict use of personal health plan information, the Plan has made the following determination [check one (1)]:

☐ Request Approved

☐ Request Denied

Name of Plan Representative

Signature of Plan Representative

Date of Determination

Part III - Termination of a Request for Restricted Use of Personal Health Plan Information

Form Part III Prepared by

Date Part III
Issued

The Plan is providing you with notice that it is terminating its agreement to restrict its use and disclosure of personal health plan information as documented above in Part II of this Form. Any personal health plan information created or received on or after **[Date of Mailing]** will not be subject to the restriction. The Plan may use and disclose your personal health plan information as permitted by law.

Name of Plan Representative

Signature of Plan Representative

Date of Determination

d. Request for Confidential Communications

Instructions for Responding to a Request for Confidential Communications

Directions for CSU:

Providing Form. If any person wishes to request that the Plan (for any plan coverage) use an alternative means to communicate his or her personal health plan information or that he or she receive personal health plan information at an alternate location, the Campus Privacy Contact should provide the person with this Form. Examples of alternative means could include mail instead of fax, phone instead of mail, etc.

Receiving a Completed Form. Upon receipt of this Form, the Campus Privacy Contact must verify that Part I (Request for Confidential Communications of Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting the Confidential Communications of personal health plan information is not the subject of the information, the Campus Privacy Contact should verify the identity and authority of the person and follow the procedures detailed in Section 4.03.

If Part I of the Form is incomplete, the Campus Privacy Contact should return it to the person for completion. Once Part I of the Form is complete, the Campus Privacy Contact should forward it to the Privacy Official.

Determination of Request. Upon receipt of this Form with Part I properly completed, the Privacy Official will respond by completing Part II (Determination of Request for Confidential Communications of Personal Health Plan Information), within the timeframes detailed in Section 6.05 of the Manual.

Part I - Request for Confidential Communications of Personal Health Plan Information

Form Received By

Date

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations. If the Payment of benefits is affected by this request, the Plan may also deny this request unless you contact the Privacy Official to discuss alternative Payment means.

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Records You Are Requesting	2a. Relationship to Employee Self <input type="checkbox"/> Spouse <input type="checkbox"/> Child <input type="checkbox"/> Other <input type="checkbox"/>
3. Your Name	3a. Your Relationship to Person in Box 2 Self <input type="checkbox"/> Spouse <input type="checkbox"/> Parent <input type="checkbox"/> Child <input type="checkbox"/> <input type="checkbox"/> Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

I am requesting that communication of personal health plan information for the person in Box 2 be provided by alternative means or at alternative locations. I [check one (1)] [☐ am ☐ am not] making this request because disclosure of all or part of the information to which the request pertains could endanger me, or the person I represent.

Please send the information by the following alternative means:

Please send the information to the following alternative address, if different than address above:

Street address _____
City, State and Zip code _____
Phone _____
Other _____

If this request relates to communication regarding Payment for health care services, please indicate how we can reach you to discuss alternative Payment means.

Signature

Date

Part II - Determination of Request for Confidential Communications of Personal Health Plan Information

Form Part II Prepared By

Date Part II
Issued

After reviewing your request for Confidential Communications of personal health plan information, the Plan has made the following determination **[check one (1)]**:

☐ **Request Approved** (see section A below)

☐ **Request Denied** (see section B below)

Section A: Request Approved

The Plan accepts your written request for the use of alternative means or alternative locations for Confidential Communications of personal health plan information. The Plan will send personal health plan information **[check all that apply]**:

☐ By the alternative means you specified in Part I; and/or

☐ To the alternative address you specified in Part I.

Section B: Request Denied

The Plan denies your written request for the use of alternative means or alternative locations for Confidential Communications of personal health plan information for the following reasons **[check all that apply]**:

☐ The Plan has determined that the request is incomplete.

☐ The Plan has determined that the request is not reasonable

☐ The request does not clearly state that the Plan's usual means or locations of disclosure of personal health plan information poses a danger to you (or to the person in Box 2).

Name of Plan Representative

Signature of Plan Representative

Date of Determination

e. Accounting of Non-Routine Disclosures

Instructions for Responding for Accounting of Non-Routine Disclosures of PHI

Directions for CSU:

Providing Form. If any person wishes to request an accounting of non-routine PHI disclosures regarding the HCRA Plan or the external EAPs, the Campus Privacy Contact should provide the person with this Form and a copy of the Privacy Notice detailing the non-routine disclosures.

Receiving a Completed Form. Upon receipt of this Form, the Campus Privacy Contact must verify that Part I (Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting personal health plan information is not the subject of the information, the Campus Privacy Contact should verify the identity and authority of the person and follow the procedures detailed in Section 4.03.

If part I of the Form is incomplete, the Campus Privacy Contact should return it to the person for completion. Once Part I of the Form is complete, the Campus Privacy Contact should forward it to the Privacy Official.

Determination of Request. Upon receipt of the Form with Part I properly completed, the Privacy Official will respond by completing Part II (Determination of Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information), within the timeframes detailed in Section 6.06 of the Manual.

If the Plan is required to temporarily suspend a person's right to receive an accounting, as detailed in Section 6.06, the Campus Privacy Contact must provide the person requesting the accounting with the appropriate information after the suspension of this person's right to receive the accounting has been lifted.

Part I - Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information

Form Received By _____

Date _____

You have the right to a list of certain disclosures the HCRA or other group health plan sponsored by the California State University (collectively, the "Plan") has made of your health information. This is often referred to as an "accounting of disclosures." You generally may receive an accounting of disclosures if the disclosure is required by law, in connection with public health activities, or in similar situations as described in more detail in the Plan's Privacy Notice.

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	
2. Name of Person Whose Accounting You Are Requesting	2a. Relationship to Employee Self <input type="checkbox"/> Spouse <input type="checkbox"/> Child <input type="checkbox"/> Other <input type="checkbox"/>
3. Your Name	3a. Your Relationship to Person in Box 2 Self <input type="checkbox"/> Spouse <input type="checkbox"/> Parent <input type="checkbox"/> Child <input type="checkbox"/> <input type="checkbox"/> Other (please describe relationship):
4. Mailing Address for Records	4a. City, State, Zip Code

I understand that I can request an accounting of non-routine disclosures of personal health plan information once within any twelve (12)-month period, free of charge. If I request accountings more frequently, I understand the Plan will charge me a reasonable, cost-based fee for each subsequent request.

The accounting of non-routine disclosures of PHI will include the following information:

- The date of disclosure;
- The name of the person or entity to whom information was made and the person's or entity's address (if known);
- A brief description of the information disclosed; and
- The reason for the disclosure.

I hereby request an accounting of any non-routine disclosures of personal health plan information of the person named in Box 2 made by the Plan for the following time period _____ [Enter time period (disclosures can be requested for a time period of up six (6) years, beginning no earlier than April 14, 2004 for the EAP and the HCRA plans)].

Signature _____

Date _____

Part II - Determination of Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information

Form II Prepared
By

Date Form II
Issued

After reviewing your request for an accounting of non-routine disclosures of personal health plan information, the Plan has made the following determination [check one(1)]:

- ☐ Request Approved without a fee (see section A below)
- ☐ Request Approved with a fee (see section B below)
- ☐ Request Denied (see section C below)

Section A: Request Approved without a Fee

Your request for an accounting of non-routine disclosures of personal health plan information is approved.

Your requested accounting of disclosures is attached to this form. There is no charge for processing request.

Section B: Request Approved with a Fee

Your request for an accounting of non-routine disclosures of personal health plan information is approved.

You requested and received an accounting of non-routine disclosures of personal health plan information, free of charge on _____ [insert date that last free of charge accounting was disclosed]. The charge for processing this request is \$ _____ [insert fee], as a fee for the preparation of your request for an accounting. You have the right to withdraw or modify your request for an accounting. Unless you contact the Privacy Official the following address _____ within 10 days from _____ [insert date] to withdraw or modify your request, the Privacy Official will mail you your requested accounting and will send you a bill for _____ which you agreed to pay by signing Part I of this form.

Section C: Request Denied

Your request for an accounting of non-routine disclosures of personal health plan information is denied because none of your PHI was disclosed for a non-routine purpose.

If you wish to make a complaint, please contact the Privacy Official at _____ [insert phone number].

Name of Plan Representative

Signature of Plan Representative

Date of Determination

f. Authorization for Use and/or Disclosure of Health Information

Directions for CSU for Using Model Authorization Form

Providing Form. If any person wishes to request an Authorization for the use or disclosure of PHI in the CSU's health plans (including the HCRA Plan), the Campus Privacy Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form, the Campus Privacy Contact should initial and date the top right corner and must verify that the Form has been properly completed.

If the person submitting the Form is not the subject of the PHI, the Campus Privacy Contact should verify the identity and authority of the person and follow the procedures detailed in Section 4.03.

This model Authorization Form is intended to allow a person to have health information sent from CSU's health plan (including its Business Associates, health insurance carriers and HMOs) to a third party for non-health plan purposes, including CSU. CSU may want to modify the specific options described in Sections A – D of this Form to reflect the most common types of requests that occur for its plans.

The "Your Rights" section includes optional language. The first option assumes Payment, enrollment, and eligibility decisions are not conditioned on the signing of an Authorization. The second option says the Plan may require Authorizations prior to a person's enrollment to make enrollment/eligibility determinations or underwriting or risk rating determinations. The appropriate option should be selected, to reflect CSU's practices.

CSU could also amend this Form to be used by CSU or an individual in requesting PHI from another covered entity in cases when an Authorization is required (either by the HIPAA privacy rule or that Covered Entity). However, the other Covered Entity is likely to require the use of its own Authorization Form.

This model Authorization Form complies with the requirements of the Health Insurance Portability and Accountability Act (HIPAA). State laws may impose additional requirements. CSU should review this form and state law issues with counsel.

Instructions for the Individual Completing this Authorization Form

- The HCRA plan and other group health plans sponsored by CSU (collectively, the “Plan”) cannot use or disclose your health information (or the health information of your children or other people on whose behalf you can act) for certain purposes without your Authorization. This form is intended to meet the Authorization requirement.
- You must respond to each section, and sign and date this form, in order for the Authorization to be valid.
- If you wish to authorize the use and/or disclosure of any notes the Plan may have that were taken by a mental health professional at a counseling session, along with other health information, you must complete one (1) form for the counseling session notes and one (1) separate form for other health information.
- The sample responses given for each section below are not exhaustive and are meant for illustrations only. Under HIPAA, there are no limitations on the information that can be authorized for disclosure.

Section A: Health Information to be Used or Released. Describe in a specific and meaningful way the information to be used or released. Example descriptions include medical records relating to my appendectomy, my laboratory results and medical records from [date] to [date], or the results of the MRI performed on me in July 1998.

Section B: Person(s) Authorized to Use and/or Receive Information. Provide a name or specific identification of the person, class of persons, or organization(s) authorized to use or receive the health information described in Section A.

Section C: Purpose(s) for which Information will be Used or Released. Describe each purpose for which the information will be used or released. If you initiate the Authorization and do not wish to provide a statement of purpose, you may select “at my request.”

Section D: Expiration. Specify when this Authorization will expire. For example, you may state a specific date, a specific period of time following the date you signed this Authorization Form, or the resolution of the dispute for which you’ve requested assistance.

Signature Line. If you are authorizing the release of somebody else’s health information, then you must describe your authority to act for the Individual.

The CSU HIPAA AUTHORIZATION FORM
Authorization to Use and/or Disclose Personal Health Plan Information

FORM RECEIVED BY DATE

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	1c. Employee Address and Phone Number
2. Name of Person Whose Health Information is the Subject of this Authorization	2a. Relationship to Employee <div style="display: flex; justify-content: space-around; margin-top: 5px;"> Self <input type="checkbox"/> Spouse <input type="checkbox"/> Child <input type="checkbox"/> Other <input type="checkbox"/> </div>
3. Your Name	3a. Authority <p>If you are not the person in Box 2, please describe your authority to act on his or her behalf:</p> <div style="border-bottom: 1px solid black; height: 20px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 20px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 20px;"></div>
4. Mailing Address for Records	4a. City, State, Zip Code

I hereby authorize _____ [Insert name of the insurance carrier, HMO, health plan vendor or the CSU Group Health and HCRA Plans who will be disclosing the health information] to use and/or disclose the health information described in Sections A — E below.

Section A: Health Information to be Used and/or Disclosed.

Specify the health information to be released and/or used, including (if applicable) the time period(s) to which the information relates. Select only one (1) of the following boxes:

- ☐ All of my health information, including, but not limited to, dates of service, types of service, treatment charts, x-rays, provider notes or other information, related to the following health condition: _____ (please describe).
- ☐ All of my health information relating to Claim Number _____, including, but not limited to, dates of service, types of service, treatment charts, x-rays, provider notes or other information.
- ☐ Other (please specify). _____

Section B: Person(s) Authorized to Use and/or Receive Information.

Specify the persons or class of persons authorized to use and/or receive the health information described in Section A:

Section C: Purposes for Which Information will be Used or Disclosed.

Specify each purpose for which the health information described in Section A may be used or disclosed. Select all of the applicable boxes below:

- ☐ To facilitate the resolution of a claim dispute.
- ☐ As part of my application for leave under the Family and Medical Leave Act (FMLA) or state family leave laws.
- ☐ For a disability coverage determination.
- ☐ At my request.
- ☐ Other (please specify) _____

Section D: Expiration of Authorization

Specify when this Authorization expires. (Provide a date or triggering event related to the use or disclosure of the information.)

- ☐ On the following date: _____.
- ☐ Upon the passage of the following amount of time: _____.
- ☐ Upon my disenrollment from the CSU Group Health and HCRA Plans.
- ☐ Upon my return from FMLA leave.
- ☐ Other (please specify) _____

Your rights:

- You can revoke this Authorization at any time by submitting a written revocation to the campus benefits office.
- A revocation will not apply to information that has already been used or disclosed in reliance on the Authorization.
- Once the information is disclosed pursuant to this Authorization, it may be re-disclosed by the recipient and the information will no longer be protected by HIPAA.
- The Plan may not condition treatment, payment, enrollment or eligibility for benefits on whether I sign the Authorization.
- You will be provided with a copy of this Authorization Form, after signing, if the Plan sought the Authorization.

Signature of Participant

Date

11.07 Breach Report Forms

The following forms are included in this section:

10.09(a) Breach Incident Report Form

10.09(b) Breach Incident Log

a. Breach Incident Report Form**Directions for CSU for Using Breach Incident Report Form**

Use of Form. As described in Section 4.07, the Plan must investigate incidents of impermissible access, uses, or disclosures of PHI which may compromise the privacy or security of the information. The purpose of this Form 10.09(a) is to collect facts about such confirmed or potential incidents. CSU workforce members aware of such incidents use this Form 10.09(a) to submit information to the Breach Contact, or use it as a guide to an oral conversation when disclosing relevant facts to the Breach Contact upon discovery of an incident requiring urgent intervention.

Receiving a Completed Form. Upon receipt of this Form the Breach Contact (or his or her designee) should initial and date the top right corner and must verify that the Form has been properly completed. All reported incidents should be investigated and the applicable procedures detailed in Section 6.05 followed to completion.

This model Breach Incident Report Form captures the types of information needed to initiate the mitigation requirements of the Health Insurance Portability and Accountability Act (HIPAA). State laws may impose additional information gathering or mitigation measures.

Breach Incident Report Form

Form Received By _____

Date _____

Please fill out this Form completely and send to the following CSU official who has been designated as the Plan's Breach Contact. If the incident is ongoing or otherwise requires immediate intervention, please call the Breach Contact at the telephone number provided:

Michelle Hamilton, Manager, Benefits and HR Programs; e-mail and fax a copy to: mhamilton@calstate.edu, facsimile 562-951-4954. Telephone number: 562-951-4413 or 562-951-4411.

Section A:

1. Reporting Staff Member Name	1a. Staff Member Daytime Telephone Number
1b. Staff Member Department/Geographical Location	
2. Is this a confirmed or suspected breach? <input type="checkbox"/> Confirmed <input type="checkbox"/> Suspected	2a. Is this an ongoing breach? <input type="checkbox"/> Yes <input type="checkbox"/> No
3. Do you believe this to be an intentional or an accidental use or disclosure? <input type="checkbox"/> Intentional <input type="checkbox"/> Accidental	3a. Please estimate the number of individuals whose PHI might be affected <input type="checkbox"/> 500 or more <input type="checkbox"/> Fewer than 500 More specific estimate number, if possible: _____
4. Date the incident was discovered _____ MM / DD / YY	4a. Date (or date range) the incident occurred _____ Starting MM/DD/YY Ending MM/DD/YY

Section B: Type of Breach

Select the type of breach incident you are reporting. If selecting the "Other" category, provide a short description in the blank field at the end of this section B **[check all that apply]**:

<input type="checkbox"/> Theft	<input type="checkbox"/> Unknown
<input type="checkbox"/> Loss	<input type="checkbox"/> Other
<input type="checkbox"/> Improper Disposal	Please describe "Other" _____
<input type="checkbox"/> Unauthorized Access	_____
<input type="checkbox"/> Hacking/IT Incident	_____

Section C: Location of Breached Information

Select the location of the PHI at the time of the breach. If selecting the "Other" category, provide a short description in the blank field at the end of this section C **[check all that apply]**:

--

Section D: Type of PHI Involved in the Breach

Select the type of PHI involved in the breach. If selecting the "Other" category, provide a short description in the blank field at the end of this section D **[check all that apply]**:

☐ Demographic information

☐ Other

☐ Financial information

Please describe "Other" _____

☐ Clinical information

Section E: Brief Description of the Breach

Please summarize the breach incident, including the geographical area and the specific IT systems/servers/applications involved, as well as any information about internal or external parties involved in the incident:

Signature

Date

b. Breach Incident Log**Directions for CSU for Using Breach Incident Log**

Use of Form. CSU workforce members use this Form 10.09(b) to record information about breach incidents reported to CSU affecting, or suspected of affecting, the Plan's PHI. The log is updated as the Breach Contact (or his or her designee) investigate breach incidents and implement the mitigation procedures described in Section 6.05.

This model Breach Incident Log captures the types of information needed to document the breach incidents reported by workforce members of CSU and submit relevant information to HHS about logged incidents for which a submission is required. This log is designed to address breach documentation needs under the Health Insurance Portability and Accountability Act (HIPAA). State laws may impose additional information gathering or documentation measures.

Plan Year _____

A	B	C	D	E	F	G	H	I	J	K		
Event #	Event Date or Range	Date Event Discovered	Approx. # of People Affected	Type of Event	Location of Event	Type of PHI Involved in Event	Safeguards in Place Before Event	Actions taken in response to event	Date(s) Individual notice provided	Was substitute notice required	Was media notice required?	Date Incident Reported to HHS
	m/d/y	m/d/y	x,xxx	√ all applicable	√ all applicable	√ all applicable	√ all applicable	√	m/d/y	Y/N	Y/N	Y/N
1				<input type="checkbox"/> Theft <input type="checkbox"/> Loss <input type="checkbox"/> Improper Disposal <input type="checkbox"/> Unauthorized Access <input type="checkbox"/> Hacking/IT Event <input type="checkbox"/> Unknown <input type="checkbox"/> Other ¹	<input type="checkbox"/> Laptop <input type="checkbox"/> Desktop Computer <input type="checkbox"/> Network Services <input type="checkbox"/> Email <input type="checkbox"/> Other Portable Electronic Device <input type="checkbox"/> Electronic Medical Record <input type="checkbox"/> Paper <input type="checkbox"/> Other ²	<input type="checkbox"/> Demographic Information <input type="checkbox"/> Financial Information <input type="checkbox"/> Clinical Information <input type="checkbox"/> Other ³	<input type="checkbox"/> Firewalls <input type="checkbox"/> Packet Filtering <input type="checkbox"/> Secure Browser Sessions <input type="checkbox"/> Strong Authentication <input type="checkbox"/> Encrypted Wireless <input type="checkbox"/> Physical Security <input type="checkbox"/> Logical Access Control <input type="checkbox"/> Antivirus Software <input type="checkbox"/> Intrusion Detection <input type="checkbox"/> Biometrics	<input type="checkbox"/> Enhanced Security and/or Privacy Safeguards <input type="checkbox"/> Mitigation of Resulting Harm <input type="checkbox"/> Sanctions of Relevant Workforce members <input type="checkbox"/> Enhanced Policies and Procedures <input type="checkbox"/> Other ⁴				
Briefly describe Event #1 (please specify if the breach occurred at or by a Business Associate):												

¹ Explain Column E “Other”: _____

² Explain Column F “Other”: _____

³ Explain Column G “Other”: _____

⁴ Explain Column I “Other”: _____

Privacy Notice

Please carefully review this notice. It describes how medical information about you may be used and disclosed and how you can get access to this information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes numerous requirements on the use and disclosure of individual health information by employer health plans. This information, known as protected health information, includes almost all individually identifiable health information held by a plan – whether received in writing, in an electronic medium, or as an oral communication. This notice describes the privacy practices of the following group health plans: health care reimbursement account and employee assistance plans. The plans covered by this notice may share health information with each other if necessary, to carry out treatment, payment, or health care operations. These plans are collectively referred to as the Plan in this notice, unless specified otherwise.

The Plan's duties with respect to health information about you

The Plan is required by law to maintain the privacy of your health information and to provide you with this notice of the Plan's legal duties and privacy practices with respect to your health information. If you participate in an insured plan option, you will receive a notice directly from the Insurer. It's important to note that these rules apply to the Plan, not California State University as an employer – that's the way the HIPAA rules work. Different policies may apply to other California State University programs or to data unrelated to the Plan.

How the Plan may use or disclose your health information

The privacy rules generally allow the use and disclosure of your health information without your permission (known as an authorization) for purposes of health care treatment, payment activities, and health care operations. Here are some examples of what that might entail:

- **Treatment** includes providing, coordinating, or managing health care by one or more health care providers or doctors. Treatment can also include coordination or management of care between a provider and a third party, and consultation and referrals between providers. *For example, the Plan may share your health information with physicians who are treating you.*
- **Payment** includes activities by this Plan, other plans, or providers to obtain premiums, make coverage determinations, and provide reimbursement for health care. This can include eligibility determinations, reviewing services for medical necessity or appropriateness, utilization management activities, claims management, and billing; as well as “behind the scenes” plan functions such as risk adjustment, collection, or reinsurance. *For example, the Plan may share information about your coverage or the expenses you have incurred with another health plan in order to coordinate payment of benefits.*
- **Health care operations** include activities by this Plan (and in limited circumstances other plans or providers) such as wellness and risk assessment programs, quality assessment and improvement activities, customer service, and internal grievance resolution. Health care operations also include vendor evaluations, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, and business planning and development. *For*

example, the Plan may use information about your claims to audit the third parties that approve payment for Plan benefits.

The amount of health information used, disclosed or requested will be limited and, when needed, restricted to the minimum necessary to accomplish the intended purposes, as defined under the HIPAA rules. If the Plan uses or discloses PHI for underwriting purposes, the Plan will not use or disclose PHI that is your genetic information for such purposes. The Plan may contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you, as permitted by law.

How the Plan may share your health information with California State University

The Plan, or its health insurer or HMO, may disclose your health information without your written authorization to California State University for plan administration purposes. California State University may need your health information to administer benefits under the Plan. California State University *agrees* not to use or disclose your health information other than as permitted or required by the Plan documents and by law. Chancellor's Office HR staff and campus HR and benefit officers are the only California State University employees who will have access to your health information for plan administration functions.

Here's how additional information may be shared between the Plan and California State University, as allowed under the HIPAA rules:

- The Plan, or its insurer or HMO, may disclose "summary health information" to California State University **if** requested, for purposes of obtaining premium bids to provide coverage under the Plan, or for modifying, amending, or terminating the Plan. Summary health information is information that summarizes participants' claims information, from which names and other identifying information have been removed.
- The Plan, or its insurer or HMO, may disclose to California State University information on whether an individual is participating in the Plan or has enrolled or disenrolled in an insurance option or HMO offered by the Plan.

In addition, you should know that California State University cannot and will not use health information obtained from the Plan for any employment-related actions. However, health information collected by California State University from other sources, for example under the Family and Medical Leave Act, Americans with Disabilities Act, or workers' compensation is *not* protected under HIPAA (although this type of information may be protected under other federal or state laws).

Other allowable uses or disclosures of your health information

In certain cases, your health information can be disclosed without authorization to a family member, close friend, or other person you identify who is involved in your care or payment for your care. Information about your location, general condition, or death may be provided to a similar person (or to a public or private entity authorized to assist in disaster relief efforts). You'll generally be given the chance to agree or object to these disclosures (although exceptions may be made – for example, if you're not present or if you're incapacitated). In addition, your health information may be disclosed without authorization to your legal representative.

The Plan also is allowed to use or disclose your health information without your written authorization for the following activities:

Workers' compensation	Disclosures to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with the laws
Necessary to prevent serious threat to health or safety	Disclosures made in the good-faith belief that releasing your health information is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety, if made to someone reasonably able to prevent or lessen the threat (or to the target of the threat); includes disclosures to help law enforcement officials identify or apprehend an individual who has admitted participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody
Public health activities	Disclosures authorized by law to persons who may be at risk of contracting or spreading a disease or condition; disclosures to public health authorities to prevent or control disease or report child abuse or neglect; and disclosures to the Food and Drug Administration to collect or report adverse events or product defects
Victims of abuse, neglect, or domestic violence	Disclosures to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or domestic violence, as required by law or if you agree or the Plan believes that disclosure is necessary to prevent serious harm to you or potential victims (you'll be notified of the Plan's disclosure if informing you won't put you at further risk)
Judicial and administrative proceedings	Disclosures in response to a court or administrative order, subpoena, discovery request, or other lawful process (the Plan may be required to notify you of the request or receive satisfactory assurance from the party seeking your health information that efforts were made to notify you or to obtain a qualified protective order concerning the information)
Law enforcement purposes	Disclosures to law enforcement officials required by law or legal process, or to identify a suspect, fugitive, witness, or missing person; disclosures about a crime victim if you agree or if disclosure is necessary for immediate law enforcement activity; disclosure about a death that may have resulted from criminal conduct; and disclosure to provide evidence of criminal conduct on the Plan's premises
Decedents	Disclosures to a coroner or medical examiner to identify the deceased or determine cause of death; and to funeral directors to carry out their duties
Organ, eye, or tissue donation	Disclosures to organ procurement organizations or other entities to facilitate organ, eye, or tissue donation and transplantation after death
Research purposes	Disclosures subject to approval by institutional or private privacy review boards, subject to certain assurances and representations by researchers about the necessity of using your health information and the treatment of the information during a research project
Health oversight activities	Disclosures to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, and compliance with regulatory programs or civil rights laws
Specialized government functions	Disclosures about individuals who are Armed Forces personnel or foreign military personnel under appropriate military command; disclosures to authorized federal officials for national security or intelligence activities; and disclosures to correctional facilities or custodial law enforcement officials about inmates
HHS investigations	Disclosures of your health information to the Department of Health and Human Services to investigate or determine the Plan's compliance with the HIPAA privacy rule

Except as described in this notice, other uses and disclosures will be made only with your written authorization. You may revoke your authorization as allowed under the HIPAA rules. However, you can't revoke your authorization with respect to disclosures the Plan has already made. You will be notified of any unauthorized access, use or disclosure of your unsecured health information as required by law.

Your individual rights

You have the following rights with respect to your health information the Plan maintains. These rights are subject to certain limitations, as discussed below. This section of the notice describes how you may exercise each individual right. See the table at the end of this notice for information on how to submit requests.

Right to request restrictions on certain uses and disclosures of your health information and the Plan's right to refuse

You have the right to ask the Plan to restrict the use and disclosure of your health information for treatment, payment, or health care operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death – or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.

The Plan is not required to agree to a requested restriction. If the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose health information about you if you need emergency treatment, even if the Plan has agreed to a restriction.

Effective February 17, 2010, an entity covered by these HIPAA rules (such as your health care provider) or its business associate must comply with your request that health information regarding a specific health care item or service not be disclosed to the Plan for purposes of payment or health care operations if you have paid for the item or service, in full out of pocket.

Right to receive confidential communications of your health information

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations.

If you want to exercise this right, your request to the Plan must be in writing and you must include a statement that disclosure of all or part of the information could endanger you.

Right to inspect and copy your health information

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "designated record set." This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. The Plan may deny your right to access, although in certain circumstances you may request a review of the denial.

If you want to exercise this right, your request to the Plan must be in writing. Within 30 days of receipt of your request (60 days if the health information is not accessible onsite), the Plan will provide you with:

- the access or copies you requested;
- a written denial that explains why your request was denied and any rights you may have to have the denial reviewed or file a complaint; or
- a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

The Plan may provide you with a summary or explanation of the information instead of access to or copies of your health information, if you agree in advance and pay any applicable fees. The Plan also may charge reasonable fees for copies or postage.

If the Plan doesn't maintain the health information but knows where it is maintained, you will be informed of where to direct your request.

Effective February 17, 2010, you may request an electronic copy of your health information if it is maintained in an electronic health record. You may also request that such electronic health information be sent to another entity or person, so long as that request is clear, conspicuous and specific. Any charge that is assessed to you for these copies, if any, must be reasonable and based on the Plan's cost.

Right to amend your health information that is inaccurate or incomplete

With certain exceptions, you have a right to request that the Plan amend your health information in a designated record set. The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete, was not created by the Plan (unless the person or entity that created the information is no longer available), is not part of the designated record set, or is not available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal, or administrative proceedings).

If you want to exercise this right, your request to the Plan must be in writing, and you must include a statement to support the requested amendment. Within 60 days of receipt of your request, the Plan will:

- make the amendment as requested;
- provide a written denial that explains why your request was denied and any rights you may have to disagree or file a complaint; or
- provide a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

Right to receive an accounting of disclosures of your health information

You have the right to a list of certain disclosures of your health information the Plan has made. This is often referred to as an "accounting of disclosures." You generally may receive this accounting if the disclosure is required by law, in connection with public health activities, or in similar situations listed in the table earlier in this notice, unless otherwise indicated below.

You may receive information on disclosures of your health information for up to six years before the date of your request. You do not have a right to receive an accounting of any disclosures made:

- for treatment, payment, or health care operations;
- to you about your own health information;
- incidental to other permitted or required disclosures;
- where authorization was provided;
- to family members or friends involved in your care (where disclosure is permitted without authorization);
- for national security or intelligence purposes or to correctional institutions or law enforcement officials in certain circumstances; or
- as part of a “limited data set” (health information that excludes certain identifying information).

In addition, your right to an accounting of disclosures to a health oversight agency or law enforcement official may be suspended at the request of the agency or official.

If you want to exercise this right, your request to the Plan must be in writing. Within 60 days of the request, the Plan will provide you with the list of disclosures or a written statement that the time period for providing this list will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request. You may make one request in any 12-month period at no cost to you, but the Plan may charge a fee for subsequent requests. You'll be notified of the fee in advance and have the opportunity to change or revoke your request.

Right to obtain a paper copy of this notice from the Plan upon request

You have the right to obtain a paper copy of this privacy notice upon request.

Changes to the information in this notice

The Plan must abide by the terms of the privacy notice currently in effect. This notice takes effect on February 17, 2010. However, the Plan reserves the right to change the terms of its privacy policies, as described in this notice, at any time and to make new provisions effective for all health information that the Plan maintains. This includes health information that was previously created or received, not just health information created or received after the policy is changed. If changes are made to the Plan's privacy policies described in this notice, you will be provided with a revised privacy notice mailed to your home address on file.

Complaints

If you believe your privacy rights have been violated or your Plan has not followed its legal obligations under HIPAA, you may complain to the Plan and to the Secretary of Health and Human Services. You won't be retaliated against for filing a complaint. For complaints regarding the Employee Assistance Program (EAP), contact the campus benefits officer. For complaints regarding the Health Care Reimbursement Account Plan, contact CSU Systemwide Human Resources Management (HRM) at CSU Office of the Chancellor – Attention Human Resources Management, 401 Golden Shore, Long Beach, CA 90802. Complaints should be filed in writing and such written document should include a description of the nature of the particular complaint.

Contact

For more information on the Plan's privacy policies or your rights under HIPAA, contact the campus benefits office.

HIPAA Privacy and Business Associate Agreement

This Agreement is entered into this ____ day of _____, _____, between [Employer] ("Employer"), acting on behalf of [Name of covered entity/plan(s) for which vendor provides services] (the "Plan(s)"), and [Name of vendor] ("Business Associate"). The Agreement is incorporated into the [Name of vendor contract] between Employer and Business Associate, dated [Date of Contract] (the "Contract"). The parties intend to use this Agreement to satisfy the Business Associate contract requirements in the regulations at 45 CFR 164.502(e), 164.504(e) and 164.314(a), issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5) and regulations promulgated thereunder; and for further applicable HIPAA developments published after enactment of P.L. 111-5, including statutes, case law, regulations and other agency guidance. *[If there is no existing applicable vendor agreement, then this agreement will be a letter agreement between employer and the vendor.]*

1.0 Definitions

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 CFR part 160 and part 164, including sections 160.103, 164.103, 164.304 and 164.501. Notwithstanding the above, "Covered Entity" shall mean the [Name of covered entity/plan]; "Individual" shall mean the person who is the subject of the Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g); Protected Health Information shall have the meaning defined in 45 CFR 160.103, which also sets forth the definition of health information, including genetic information as clarified by P.L. 110-233 and applicable regulations; "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his designee; "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E; and "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information at 45 CFR part 160 and part 164, subparts A and C.

2.0 Obligations and activities of Business Associate

Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by Section 3.0 of this Agreement, or as required by law.

- (a) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- (b) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

- (c) Business Associate agrees to report to Covered Entity, in writing, any use or disclosure of the Protected Health Information not provided for by this Agreement and any security incident of which it becomes aware. For purposes of this Agreement, security incident” shall have the same meaning as the term “security incident” in 45 CFR 164.304
- (d) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information or electronic Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- (e) Business Associate agrees to provide access, at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations, to Protected Health Information in a designated record set, to the Covered Entity or directly to an Individual in order to meet the requirements under 45 CFR 164.524.
- (f) Business Associate agrees to make any amendment(s) to Protected Health Information in a designated record set that the Covered Entity or an Individual directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations.
- (g) Business Associate agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity, to the Secretary in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity’s compliance with the Privacy Rule.
- (h) Business Associate agrees to document disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
- (i) Business Associate agrees to provide to Covered Entity or an Individual an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528, in a prompt and reasonable manner consistent with the HIPAA regulations.
- (j) Business Associate agrees to satisfy all applicable provisions of HIPAA standards for electronic transactions and code sets, also known as the Electronic Data Interchange (EDI) Standards, at 45 CFR Part 162. Business Associate further agrees to ensure that any agent, including a subcontractor that conducts standard transactions on its behalf will comply with the EDI Standards.

- (k) Business Associate agrees to determine the minimum necessary type and amount of PHI required to perform its services and will comply with 45 CFR 164.502(b) and 514(d).
- (l) Business Associate agrees to restrict the use or disclosure of Protected Health Information, and document those restrictions, at the request of Covered Entity pursuant to 45 CFR 164.522(a), in a prompt and reasonable manner consistent with the HIPAA regulations.
- (m) Business Associate agrees to accommodate alternative means or alternative locations to communicate Protected Health Information, and document those alternative means or alternative locations, at the request of Covered Entity or an Individual, pursuant to 45 CFR 164.522(b), in a prompt and reasonable manner consistent with the HIPAA regulations.
- (n) Business Associate agrees to be the primary party responsible for receiving and resolving requests from an Individual exercising his or her individual rights described in subsections (f), (g), (j), and (n) of this section 2.0.
- (o) Business Associate agrees to implement any and all administrative, technical and physical safeguards necessary to reasonably and appropriately protect the confidentiality, integrity and availability of electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of the Plan(s).
- (p) Business Associate agrees to ensure that access to electronic Protected Health Information related to the Covered Entity is limited to those workforce members who require such access because of their role or function.
- (q) Business Associate agrees to implement safeguards to prevent its workforce members who are not authorized to have access to such electronic Protected Health Information from obtaining access and to otherwise ensure compliance by its workforce with the Security Rule.
- (r) Business Associate acknowledges that enactment of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5, ARRA) amended certain provisions of HIPAA in ways that now directly regulate, or will on future dates directly regulate, Business Associate's obligations and activities under HIPAA's Privacy Rule and Security Rule. Requirements applicable to Business Associate under Title XIII, Subtitle D of ARRA are hereby incorporated by reference into the Agreement, including provisions that would govern the Plan's action if the Business Associate undertakes that action on behalf of the Plan. Business Associate agrees to comply, as of the applicable effective dates of each such HIPAA obligation relevant to Business Associate, with the requirements imposed by ARRA, including monitoring federal guidance and regulations published thereunder and timely compliance with such guidance and regulations. In consequence of the foregoing direct regulation of Business Associate by HIPAA laws and regulations, notwithstanding any other provision of the Agreement, Business Associate further agrees to monitor HIPAA Privacy and Security requirements imposed by future laws and regulations, and to timely

comply with such requirements when acting for or on behalf of the Plan in its capacity as a Business Associate.

- (s) Further, Business Associate agrees to timely undertake all activities associated with the duties of ARRA section 13402 (and related guidance) in the event that Business Associate (or its agent) experiences a breach of Covered Entity's Protected Health Information requiring notice to affected individuals and/or any other party. Business Associate agrees that Covered Entity will be given reasonable advance opportunity to review the proposed notice or other related communications to any individual or third party regarding the breach; Covered Entity may propose revised or additional content to the materials which will be given reasonable consideration by Business Associate (or its agent).

3.0 Permitted or required uses and disclosures by Business Associate

(a) General use and disclosure.

- (i) Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Contract and in this Agreement, provided that such use or disclosure of Protected Health Information would not violate the Privacy Rule, including the minimum necessary requirement, if done by Covered Entity.
- (ii) Business Associate shall share Protected Health Information as reasonably requested by Covered Entity with Covered Entity and the Centers for Medicare and Medicaid Services (CMS), and with their agents and any other parties permitted by CMS guidance (including CMS's FAQ #5482), where the Covered Entity is submitting to CMS the Protected Health Information required by 42 CFR 423.884 for Medicare's retiree drug subsidy program.
- (iii) Business Associate shall share Protected Health Information as reasonably requested by Employer to carry out its responsibilities as plan administrator of the Plan(s), including, without limitation, for purposes of auditing the performance of Business Associate.

(b) Additional use and disclosure.

- (i) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- (ii) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that such disclosures are required by law, or Business

Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

- (iii) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide data aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).
- (iv) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

4.0 Obligation to inform Business Associate of Covered Entity's privacy practices and any authorization or restriction

- (a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.
- (b) Covered Entity shall provide Business Associate with any changes in, or revocation of, authorization by Individual or his or her personal representative to use or disclose Protected Health Information, if such changes affect Business Associate's uses or disclosures of Protected Health Information.
- (c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

5.0 Permissible requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

6.0 Term and termination

- (a) **Term.** The term of this Agreement shall be effective as of _____ [date on or after April 20, 2005 – there may be a different date depending on the effective date of the EAP contract], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to

return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

- (b) **Termination for cause.** The Covered Entity may, in its sole discretion, provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Contract if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate the Contract if Business Associate has breached a material term of this Agreement and cure is not possible. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary of Health and Human Services.
- (c) **Effect of termination.** The parties mutually agree that it is essential for Protected Health Information to be maintained after the expiration of the Agreement for regulatory and other business reasons. The parties further agree that it would be infeasible for Covered Entity to maintain such records because Covered Entity lacks the necessary system and expertise. Accordingly, Covered Entity hereby appoints Business Associate as its custodian for the safe keeping of any record containing Protected Health Information that Business Associate may determine it is appropriate to retain. Notwithstanding the expiration or termination of the Contract, Business Associate shall extend the protections of this Agreement to such Protected Health Information, and limit further use or disclosure of the Protected Health Information to those purposes that make the return or destruction of the Protected Health Information infeasible.

7.0 Miscellaneous

- (a) **Regulatory references.** A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended, and for which compliance is required.
- (b) **Amendment.** Upon the enactment of any law or regulation affecting the use, disclosure, or safeguarding of Protected Health Information or electronic Protected Health Information, or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either party may, by written notice to the other party, amend the Contract and this Agreement in such manner as such party determines necessary to comply with such law or regulation. If the other party disagrees with such amendment, it shall so notify the first party in writing within thirty (30) days of the notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, then either of the parties may terminate the Contract on thirty (30) days written notice to the other party.
- (c) **Survival.** The respective rights and obligations of Business Associate under Section 6.0 of this Agreement shall survive the termination of this Agreement.

- (d) **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy and Security Rules.
- (e) **No third party beneficiary.** Nothing expressed or implied in this Agreement or in the Contract is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assignees of the parties, any rights, remedies, obligations, or liabilities whatsoever.
- (f) **Severability.** If any provision of this Agreement is held illegal, invalid, prohibited or unenforceable by a court of competent jurisdiction, that provision shall be limited or eliminated in that jurisdiction to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.
- (g) **Governing law.** This Agreement shall be governed by and construed in accordance with the laws of the state of California to the extent not preempted by the Privacy or Security Rules or other applicable federal law.
- (h) **Indemnification and performance guarantees.** The indemnification and performance guarantee provisions contained in the Contract shall also apply to this Agreement.

[For Employer]

[For Vendor]

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Authorization to Use and/or Disclose Personal Health Plan Information

Form Received By

Date

1. Employee Name	1a. Employee Health Plan ID Number
1b. Employee Date of Birth	1c. Employee Address and Phone Number
2. Name of Person Whose Health Information is the Subject of this Authorization	2a. Relationship to Employee <div> <input type="checkbox"/> Self <input type="checkbox"/> Spouse <input type="checkbox"/> Child <input type="checkbox"/> Other </div>
3. Your Name	3a. Authority If you are not the person in Box 2, please describe your authority to act on his or her behalf:
4. Mailing Address for Records	4a. City, State, Zip Code

I hereby authorize _____ [Insert name of the insurance carrier, HMO, health plan vendor or the CSU Group Health and HCRA Plans who will be disclosing the health information] to use and/or disclose the health information described in Sections A — E below.

Section A: Health Information to be Used and/or Disclosed.

Specify the health information to be released and/or used, including (if applicable) the time period(s) to which the information relates. Select only one (1) of the following boxes:

☐ All of my health information, including, but not limited to, dates of service, types of service, treatment charts, x-rays, provider notes or other information, related to the following health condition: _____ (please describe).

☐ All of my health information relating to Claim Number _____, including, but not limited to, dates of service, types of service, treatment charts, x-rays, provider notes or other information.

☐ Other (please specify). _____

Section B: Person(s) Authorized to Use and/or Receive Information.

Specify the persons or class of persons authorized to use and/or receive the health information described in Section A:

Section C: Purposes for Which Information will be Used or Disclosed.

Specify each purpose for which the health information described in Section A may be used or disclosed. Select all of the applicable boxes below:

- ☐ To facilitate the resolution of a claim dispute.
- ☐ As part of my application for leave under the Family and Medical Leave Act (FMLA) or state family leave laws.
- ☐ For a disability coverage determination.
- ☐ At my request.
- ☐ Other (please specify) _____

Section D: Expiration of Authorization

Specify when this Authorization expires. (Provide a date or triggering event related to the use or disclosure of the information.)

- ☐ On the following date: _____.
- ☐ Upon the passage of the following amount of time: _____.
- ☐ Upon my disenrollment from the CSU Group Health and HCRA Plans.
- ☐ Upon my return from FMLA leave.
- ☐ Other (please specify) _____

Your rights:

- You can revoke this Authorization at any time by submitting a written revocation to the campus benefits office.
- A revocation will not apply to information that has already been used or disclosed in reliance on the Authorization.
- Once the information is disclosed pursuant to this Authorization, it may be re-disclosed by the recipient and the information will no longer be protected by HIPAA.
- The Plan may not condition treatment, payment, enrollment or eligibility for benefits on whether I sign the Authorization.
- You will be provided with a copy of this Authorization Form, after signing, if the Plan sought the Authorization.

Signature of Participant

Date

MERCER



MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

HR 2011-07
ATTACHMENT F

Consulting. Outsourcing. Investments.



March 9, 2010

HIPAA Privacy and Security Training

California State University

Elizabeth Marks
Kathleen Murray

Agenda

- Why HIPAA privacy and security training is important
- HIPAA privacy training
- HIPAA security training
- HIPAA breach notice rules
- HIPAA sanction policy

Why HIPAA training is important

Why HIPAA training is important to you and CSU

- You may interact with employees in many different capacities that involve discussions about medical and other sensitive employee information that needs to be safeguarded
- For example
 - Employees may willingly share information with you about their own health problems
 - Employees may ask you to help them solve problems relating to how a health or dental claim is being handled by an HMO or insurer
 - You may get involved in discipline, workers' compensation, FMLA, or disability issues that involve private medical information
- The training will explain CSU's obligations under the HIPAA Privacy requirements that apply to protected health information relating to employee health plans, and it will also reinforce the importance of maintaining the privacy of any sensitive employee information

Penalties and enforcement

New civil penalties

TYPE OF VIOLATION		PENALTY
	Each violation	All such violations of an identical provision in a calendar year
Before HITECH		
Due to any type of violation	\$100	\$25,000
After HITECH – Effective February 2009		
Due to unknowing violation	\$100 - \$50,000	\$1,500,000
Due to reasonable cause but not willful neglect	\$1,000 - \$50,000	\$1,500,000
Due to willful neglect that is timely corrected	\$10,000 - \$50,000	\$1,500,000
Due to willful neglect if not timely corrected	\$50,000	\$1,500,000

Penalties and enforcement

New enforcement

CRIMINAL PENALTIES	Then	Now
Clearly applicable to individual employees (not just the entity)	No	Yes
Penalties	Fines \$50,000 - \$250,000 1-10 years imprisonment for “knowing misuse”	

OTHER CONSEQUENCES	Then	Now
Bad publicity	Yes	Yes
Negative employee relations	Yes	Yes
Damage to business relationships	Yes	Yes

HIPAA Privacy Training Overview

HIPAA Privacy Training Agenda

- HIPAA Privacy overview
- Uses and disclosures of protected health information (PHI)
- Best practices for safeguarding PHI
- Individual rights
- HIPAA Privacy Official
- Notice of privacy practices



The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

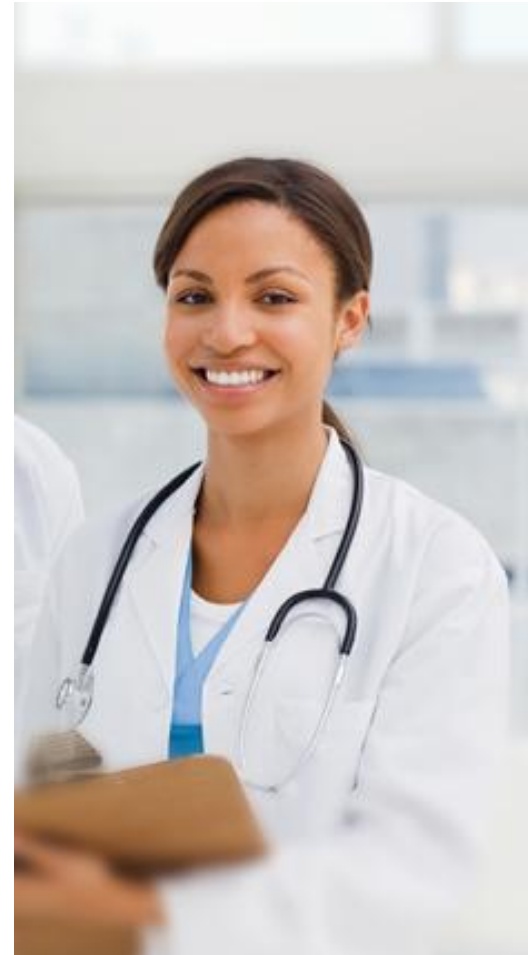
- HIPAA “administrative simplification” regulations govern the privacy and security of individual medical information used, transmitted, and retained by employer health plans and other covered entities, and the electronic transfer of certain health data
- These regulations cover the following areas:
 - **Privacy** - rules that safeguard the privacy of individuals’ health information by placing limits on its use and disclosure
 - **EDI** - rules that standardize transactions/code sets for electronic data interchange (EDI) to encourage commerce in health care
 - **Security** - rules that require the confidentiality and integrity of electronic data, prevent unauthorized access to data, and guard against physical hazards



Protected health information (PHI)

What is the definition of PHI?

- **PHI** is at the center of the HIPAA Privacy Rule. The rule closely regulates how PHI is used, disclosed, transmitted, and retained. The rule also gives individuals certain rights with respect to their PHI
- **PHI** is health information that . . .
 - Is created, received, or maintained by a covered entity, **and**
 - Includes “individual identifiers” that clearly identify an individual (or has components that reasonably 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 (new: genetic information)



Protected health information (PHI)

What are “individual identifiers”?

- What identifiers make health information PHI?
- Any combination of data could identify the individual who's the subject of the information:
 - Name
 - SSN
 - Date of birth
 - Date of hire
 - Dates of service
 - Telephone or fax numbers
 - Email address
 - Medical record number
 - Health plan beneficiary number
 - Geographic identifiers smaller than a state
 - Certificate/license numbers
 - Vehicle identifiers
 - URLs
 - IP address numbers
 - Biometric identifiers
 - Photographic image
 - Other unique identifying numbers or codes

Protected health information (PHI)

What form does PHI take and where is it found?

What form can PHI take?

- PHI can be any communication format:
 - Print
 - Electronic (including email)
 - Oral

When will you interact with PHI?

- Benefit staff frequently come into contact with PHI during:
 - Assisting employees with claims (“customer service”)
 - CSU oversight of health plans
 - Response to requests for health information

Protected health information (PHI)

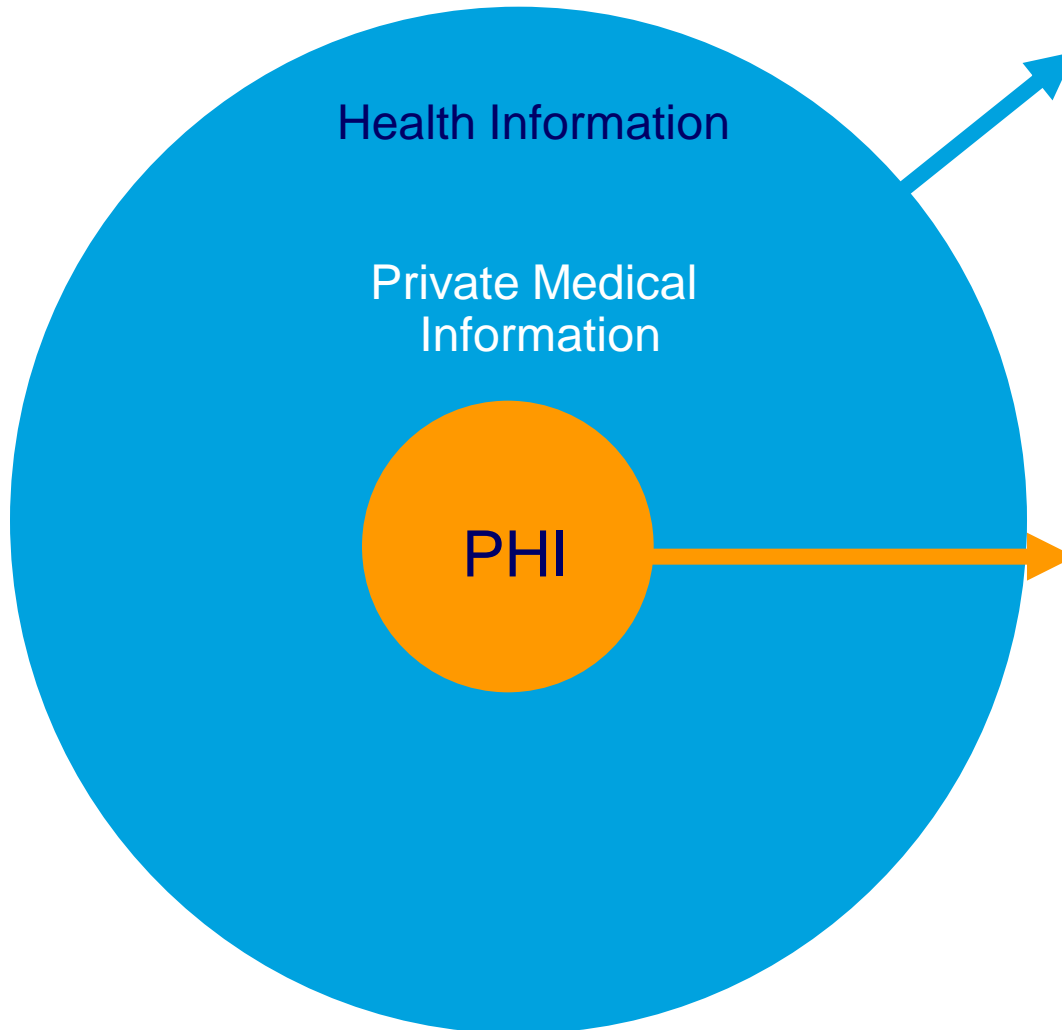
What's not considered PHI?

- Private medical information that's obtained from the employee or health care provider (but not from the health plan) for disability or employment purposes, such as
 - Short-term or long-term disability claims
 - Life insurance
 - Disability pensions
 - FMLA or other types of leave
 - Workers' compensation
 - Americans with Disabilities Act (ADA) compliance
 - 401(b) medical hardship withdrawals
- The HIPAA Privacy rule does not apply to employer interaction with these types of personal medical information
- However, other laws do protect private medical information



Protected health information (PHI)

What is (and is not) PHI?



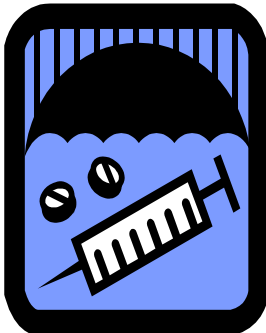
Private medical information that relates to FMLA, workers' compensation, or ADA, including health information maintained as part of employment records in CSU's role as employer is not covered by HIPAA, but still must be protected.

PHI is health information that relates to a person's medical condition, the provision of medical care, or the payment of medical care, and that is:

- Individually identifiable, and
- Created, received, or maintained by the health plans

What is a HIPAA covered entity?

- A HIPAA “covered entity” is a health plan, health care provider, or health care clearinghouse
 - Health plans, such as
 - ◆ Group health plans sponsored by CSU or PERS
 - ◆ EAPs
 - ◆ Health care reimbursement account
 - Health care providers such as doctors, hospitals
 - Health care clearinghouses that assist in transmission of ePHI
- Covered entities must comply with the standards set in the HIPAA Rule



What benefits are affected by HIPAA?

- HIPAA applies to CSU's health plans offered to employees, COBRA participants, retirees, and their families that provide or pay for:
 - Medical
 - Dental
 - Vision
 - Prescription drugs
 - Employee assistance plans
 - Health care reimbursement account (HCRA)
 - Certain wellness programs
 - Long term care
- Privacy rules apply to *both* insured and self-funded arrangements



What is CSU's responsibility under HIPAA privacy?

- CSU is responsible for complying with HIPAA privacy rules for its self-funded health plans, including EAPs and HCRA
 - Obtain business associate agreements
- CSU has limited responsibility for fully insured plans and HMOs
 - Insurers/HMOs are responsible for complying with privacy rules for insured health plans
 - However, insurers won't release PHI to CSU without individual authorization or formal assurances from CSU that CSU will protect PHI

Quiz

An employee calls to discuss her upcoming hospitalization for heart condition tests with Joe, a CSU campus benefit officer who performs health plan administrative functions.

The employee asks Joe to help her with the required pre-certification from the HMO. The HMO provides Joe with details of the surgical procedure that extend beyond the information originally given by the employee.

Question: Is the information Joe received from the HMO considered PHI?

Yes or **No**



Quiz Answer

The correct answer is **Yes.**

PHI in any form, even oral communication, relating to future treatment of a medical condition that clearly identifies an individual is PHI if it is received from the health plans.





HIPAA Privacy Training

Uses and Disclosures of PHI

Who has access to PHI?

- CSU staff responsible for administering health plans, but only to perform certain administrative functions (e.g. assistance with customer service, claims questions, data analysis)
- “Business associates” that perform services for the plans and have signed Business Associate Agreements
- Insurers and HMOs with respect to the plans they insure



When PHI *can* be used

- PHI can be used or disclosed for any purpose if the participant specifically permits the use or disclosure in a HIPAA Authorization
- A HIPAA Authorization is generally ***not*** required to use PHI for:
 - Enrollment activities
 - Normal administration of the health plans:
 - ◆ Payment activities (e.g. HCRA claims), or
 - ◆ Health care operations (e.g. audits, customer service, vendor performance reviews)
 - Obtaining premium bids and making plan amendments if only “summary health information” is used
- CSU employees must follow policies and procedures that satisfy the HIPAA Privacy standards when using PHI

When PHI *cannot* be used

Any other time!



Important definitions

- **Disclosures** – The release, transfer, or provision of access to, or divulgence in any other manner of PHI to parties **outside** the covered entity holding the information
- **Use** – The sharing, employment, application, utilization, examination, or analysis of PHI **within** the covered entity that maintains such information
- **Minimum necessary** – Covered entities must make reasonable efforts to use, request, and disclose a ‘limited data set’ of PHI unless more elements are needed to accomplish the task
- **Limited data set** – A limited data set is PHI that **excludes** the individual identifiers



What information can business associates and insurers share with CSU?

- Enrollment/disenrollment information
 - Processing of annual enrollment selections
 - ◆ New hire benefit selections
 - ◆ Enrollment changes
 - ◆ Eligibility questions
- Summary health information (all individual identifiers removed)
 - Obtain premium bids for coverage
 - Modify, amend, or terminate the plan
- Information related to plan administration activities
 - As long as CSU promises to protect the PHI via a HIPAA amendment)



Plan administration: Procedures for protecting PHI

- As required by the HIPAA Privacy Rule, CSU has identified that HR and benefits are the only staff with access to PHI
- HR and benefits staff must follow procedures to:
 - Limit disclosures of and requests for PHI to the “minimum necessary” for the intended purpose
 - Maintain procedures for storage of PHI
 - If feasible, return or destroy PHI received from the plan and follow procedures for PHI that isn’t returned or destroyed
- HR and benefits staff will not use PHI obtained as the result of health plan administration for **employer** functions (such as processing disability or life claims) unless they have written authorization from the plan participant

Non-plan administration activities

Individuals who are not identified to perform health plan administrative functions must have a written HIPAA Authorization from the plan participant to receive PHI from the health plan

PHI will not be used or disclosed on the basis of a written HIPAA Authorization, unless it is verified that the Authorization:

- Has not expired,
- Has not been revoked, and
- Includes all required information

A copy of each Authorization will be retained for six years from the later of the date the authorization was created or the last date the authorization was effective

Disclosure to others acting on behalf of the participant

- Participants can generally obtain their own PHI without a HIPAA Authorization
- A participant's PHI may, and in some situations must, be provided to certain others without a HIPAA Authorization as follows:
 - Persons considered to be the participant's legal "personal representative" must be treated the same as the participant (including for purposes of individual rights in the next section)
 - Family members, friends, and others who are not a personal representative, if identified by the participant and involved with the participant's care or payment for care **and**
 - ◆ The participant had opportunity to agree or object to the disclosure, **or**
 - ◆ The participant's incapacity or an emergency makes it impossible to obtain the participant's agreement

Who can be a “personal representative”?

- Personal representatives of a participant who may obtain the participant’s PHI without the need for a HIPAA Authorization generally may include the following:

PHI of:	May be shared with:
Minor child	Parent or guardian*
Adult child	Parent or guardian**
Adult	Spouse or adult**
Deceased	Executor or administrator**

*proof of relationship required

**proof of legal authority required

Limitations on parent's status as personal representative

- There are some restrictions on providing PHI to a parent or guardian
 - Minor lawfully obtained the health services with consent of someone other than parent
 - Information sharing would not be in minor's best interest (endangerment, abuse, neglect)
- Refer to state laws for details



Verify the identity of all persons making requests for PHI

Who makes the request

Participants, beneficiaries, and others acting on their behalf

Health plans, providers, and other covered entities

To verify identity. obtain*

- Photo identification
- Letter or oral authorization
- Marriage certificate
- Birth certificate
- Enrollment information
- Identifying number
- Claim number
- Identifying information about the purpose of the request
- Identity of a person, business, address, phone number, and/or fax number

Verify the identity of all persons making requests for PHI (continued)

Who makes the request	To verify identity, obtain*
Public officials	<ul style="list-style-type: none">• For in-person requests, agency identification, official credentials, or other identification, or other proof of government status• For written requests, on appropriate letterhead, and written statement of legal authority
Person acting on behalf of a public official	<ul style="list-style-type: none">• Written statement on government letterhead or other evidence of agency

Verify the identity of all persons making requests for PHI (continued)

Who makes the request	To verify identity, obtain*
Person acting through legal process	<ul style="list-style-type: none">• Copy of the applicable warrant, subpoena, order, or other legal process
Person needing information based on health or safety threats	<ul style="list-style-type: none">• Consult with the Privacy Official

**Information that is NOT individually identifiable
can be used or disclosed at any time, without
restrictions.**

**Such information is referred to as
“de-identified” information.**



Quiz

CSU staff can disclose as much PHI as they like in the course of performing plan administrative functions.

True or False



Quiz Answer

The correct answer is **False.**

CSU's workforce staff must always take measures to limit the uses and disclosures of PHI to the minimum necessary to accomplish the intended purposes of a plan administrative function





HIPAA Privacy Training

Best Practices for Safeguarding PHI

Best practices for protecting PHI

- When using or disclosing PHI, the plan must make reasonable efforts to use or disclose the least amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure, or request; use de-identified information whenever possible
- The plan must make reasonable efforts to prevent uses and disclosures not permitted by the plan's Privacy and Security policies and procedures
- PHI in any medium, including paper, electronic media, oral or visual representations must be protected by physical and technical safeguards
- When a person calls for assistance on a claim issue that will involve PHI, you must verify identity before taking any other action



Protecting hard-copy PHI

- Limit photocopies that contain PHI
- Keep a clean desk
- Put away and secure PHI when you leave your desk during the day
- Keep PHI in closed, locked drawers/cabinets when you leave for the day
- Store documents you must keep for a long time in areas with limited access
- Destroy PHI as soon as it is no longer needed
- Shred all paper when no longer required



Protecting email and electronic storage media that contain PHI

- Funnel incoming email through appropriate channels to limit the number of people who have access to PHI
- Limit use of PHI in emails (avoid forwarding email strings that contain PHI; make sure message contains only the minimum necessary)
- Store diskettes, CDs, or tapes in locked rooms or files
- Destroy electronic PHI that is no longer needed (including shredding or destroying disks/CDs)
- Account for the external distribution of electronic media that contains PHI
- Permanently remove PHI from disk drives, diskettes, or tapes that will be reused
- Use locking screensavers to limit access to work stations and laptops



Protecting faxes that contain PHI

- Use fax machines designated for health plan administration
- Use fax cover sheet with confidentiality statement
- Limit faxing of PHI to urgent information only
- Notify receiver that you are sending fax
- Check confirmation sheets to verify fax was received



Protecting oral communication regarding PHI

- Limit discussion of PHI in conversations unless absolutely necessary
- Verify the identity of individuals on the phone before discussing PHI
- Use reasonable measures to prevent others from overhearing conversations (close your door and avoid speaker phone, for examples)
- Restrict voice mail messages to high-level information



Quiz

Question: Which of the following safeguards should be followed for protecting hard-copy PHI?

Choose your answer:

- a) Keep a clean desk
- b) Keep PHI in closed, locked drawers/cabinets when you leave for the day
- c) Destroy PHI as soon as it is no longer needed
- d) All of the above



Quiz Answer

The correct answer is (d).

All of the physical safeguards listed are reasonable measures to take to ensure that hard-copy PHI is kept secure and confidential





HIPAA Privacy Training

Individual Rights

Individual rights regarding PHI

- Basic rights granted by HIPAA Privacy to each person include the right to:
 - Access, inspect, and copy PHI that relates to him or her
 - Amend PHI if there are errors or omissions
 - Request restricted use of PHI
 - Require confidential communications
 - Require an accounting of non-routine disclosures
- All rights may be exercised by an individual to whom the PHI pertains or by his or her designated representative

Individual rights regarding PHI

- CalPERS medical dental or vision coverage
 - Participant requests (other than requests for restrictions or requests for alternative means or locations for receiving communications of PHI) that pertain to CalPERS medical, dental or vision coverage should be directed to the applicable HMO or insurance carrier
- HCRA and any other non-CalPERS health benefits
 - The Campus Privacy Contact will have the participant fill out the applicable form and forward it to the CSU Privacy Official. The Privacy Official will respond to all requests
 - See CSU's HIPAA Privacy Policy and Procedure Manual for further information

HIPAA Privacy Training

HIPAA Privacy Official

HIPAA Privacy Official: roles and responsibilities

- CSU's HIPAA Privacy Official is Michelle Hamilton
- The Privacy Contacts are the campus Benefit Officers
- The Privacy Official is responsible for the HIPAA Privacy compliance process, including:
 - Assessing CSU's HIPAA Privacy compliance needs
 - Developing and implementing HIPAA-related policies and procedures, including those in the HIPAA Privacy Manual
 - Supervising training for CSU's staff involved in health plan administration
- Other duties of the HIPAA Privacy Official include:
 - Monitoring ongoing compliance
 - Monitoring resolution and tracking of complaints
 - Determining appropriate actions to take to resolve complaints
 - Answering HIPAA-related questions for CSU's employees
 - Ensuring that required documentation is maintained and retained for six years



HIPAA Privacy Training

Notice of Privacy Practices

Notice of privacy practices

- Describes CSU's written procedures for uses and disclosures that are part of CSU's health plan administration
- Lists uses and disclosures of PHI that the plan can make without an authorization (e.g. responding to a request from a public health agency)
- Describes CSU's process for handling participant requests for PHI, complaints about alleged privacy violations, and other HIPAA individual rights
- Lists contacts with business associates that will provide assistance to plan participants who assert their HIPAA Privacy rights
- Must be given to new participants at enrollment, and to all within 60 days of a material revision

HIPAA Security Training

HIPAA Security Awareness Training

- The security regulations (HIPAA Security Rule) generally require employers who sponsor group health plans to take appropriate precautions to secure their health plans' electronic protected health information.
- We are providing this Security Awareness Training to educate you on the general provisions of the HIPAA Security Rule and to apprise you of the basic precautions you will be expected to observe to assist CSU in satisfying its responsibilities under the regulations.
- Should you have any questions about this training course, or your participation in it, please contact your HIPAA Security Official.

What will be covered in this training?

This course will discuss the following subject areas:

- How this training relates to you
- Overview of the HIPAA Security Rule
- Three areas that the HIPAA Security regulations indicate are critical in maintaining the security of electronic Protected Health Information (e-PHI)
 - Minimizing the introduction of malicious computer software
 - Proper use of system user names
 - Creating and maintaining robust passwords
- Additional responsibilities for e-PHI users



Why is HIPAA Security Awareness Training mandatory?

Because you are an employee who has access to computer equipment or software containing protected health information related to CSU's health plans, the HIPAA Security Rule requires that you participate in HIPAA Security Awareness Training to learn about the basic procedures you must follow to protect that information.

Following CSU's electronic security procedures is important because the procedures help to protect the:

- Confidentiality (only the right people see it),
- Integrity (the information is what it is supposed to be—there has been no unauthorized alteration or destruction), and
- Availability (the right people can see it when needed)

HIPAA Security Training Overview

HIPAA Security Rule

- Electronic PHI (or e-PHI) is PHI:
 - Electronically created;
 - Electronically received;
 - At rest or maintained in a storage device such as a computer hard drive, disk, CD, or tape; or
 - In transit via the Internet, dial-up lines, etc.
 - ◆ For example, email FTP (file transfer protocol), EDI (electronic data interchange), IVR (interactive voice response), and fax-back systems used to transmit PHI



HIPAA Security Rule

- e-PHI is not:
 - PHI that was not in electronic form before transmission, such as information shared by:
 - ◆ Person-to-person telephone calls,
 - ◆ Copy machines,
 - ◆ Paper-to-paper fax machines, or
 - ◆ Most voice mail
 - De-identified information is not PHI or e-PHI
- The HIPAA Privacy Rule establishes standards for safeguarding e-PHI only



What are the objectives of the HIPAA Security Rule?

- Secure e-PHI at rest, while in the custody of group health plans
- Secure e-PHI in transit, both between health plans
- Protect against reasonably anticipated:
 - Threats or hazards to e-PHI security or integrity
 - Unauthorized uses or disclosures



HIPAA Security Rule Required Policies and Procedures

- The HIPAA Security Rule requires that CSU implement reasonable and appropriate *policies and procedures* governing administrative, physical, and technical safeguards to comply with the HIPAA Security Rule
- Procedures implemented to comply with the HIPAA Security Rule must be reviewed and modified, as needed, to ensure the reasonable and appropriate protection of e-PHI over time.
- HIPAA Security compliance is an on-going effort that must be constantly monitored
- You should review CSU's HIPAA Security policies and procedures for more detail about the safeguards we've implemented to protect e-PHI. Contact the CSU HIPAA Security Official for these policies and procedures



HIPAA Security Training

Critical Security Risks

Critical Security Risks

Three critical security risks must be eliminated or minimized by all CSU staff who have access to e-PHI to ensure the confidentiality, availability, and integrity of e-PHI.

1. Malicious computer software, such as viruses
2. Unauthorized use of system user names
3. Weak or unprotected system and file passwords



Risk 1: Malicious Computer Software

- Malicious computer software:
 - Is designed to damage or disrupt a system
 - Has an intentional negative impact on the confidentiality, availability, or integrity of e-PHI
- Malicious computer software can:
 - Destroy your computer files, or
 - Block your access to critical computer applications



Malicious Software

How does it get on my computer?

- Infected e-mail attachments
- Computer software from non-secure sources
 - Websites
 - Unlicensed software
- Files stored on external electronic storage media
 - Diskettes or CDs could contain malicious software



Malicious Software

Your responsibilities to safeguard against it

- ***Be suspicious!*** Don't open e-mails or e-mail attachments that are from suspicious or unknown sources or have suspicious subjects
- ***Report suspicious e-mail*** and other potential security incidents to the CSU HIPAA Security Official or IT staff
- ***Comply*** with CSU instructions to ensure your work- station virus protection software is kept up-to-date
- ***Read*** security alerts released by IT staff on the status of malicious software threats related to e-mails



Malicious Software

Your responsibilities to safeguard against it

- ***Never*** copy, download, or install computer software without permission
- ***Never*** disable or tamper with the virus protection software installed on your workstation and/or laptop
- ***Always scan*** files from external storage media *before copying* them to detect the presence of malicious software
- ***Promptly notify*** the IT staff if you become aware of *any* misuse of CSU equipment, software, or data within CSU
- ***Make sure*** any home workstation or laptop you utilize for CSU business has up-to-date virus protection software

Security Alerts and Reminders

Why read them?

- **Security alerts** issued by the IT staff contain important information and instructions about how to safeguard against new sources of malicious software threats
- **Security reminders** contain important suggestions and methods of improving your ability:
 - To safeguard against malicious software threats, and
 - To maintain secure individual system-user names and password



Quiz

Question:

How often should the computer virus software on my workstation or laptop be updated?

Choose your answer:

- a) Never. Once installed, it never needs to be updated
- b) As soon as the updates are available
- c) Only after a security incident related to malicious software has occurred



Quiz Answer

The correct answer is (b).

Computer virus protection software should be kept as up-to-date as possible in order to ensure that the appropriate safeguards are in place to protect against the new and ever-changing malicious software threats that are present.



Quiz

Question:

If you receive a security reminder or security alert in your e-mail in-box, you should:

Choose your answer:

- a) Delete it without reading its contents
- b) Immediately open the e-mail, read it, and follow all of the instructions
- c) If you are busy, open and read it later
- d) Follow the instructions, but only if you think they apply to you



Quiz Answer

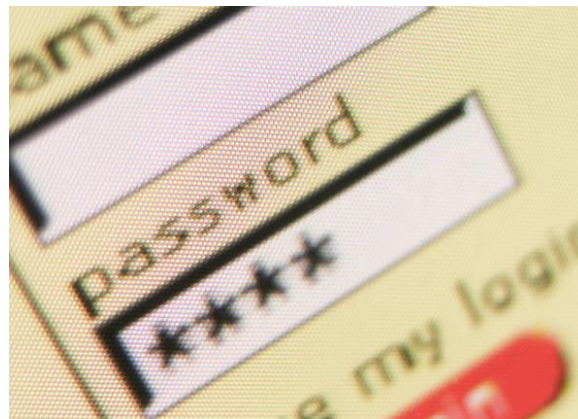
The correct answer is (b).

The purpose of security reminders and alerts is to assist in preventing malicious software attacks. By paying immediate attention to the instructions contained in the security reminders and alerts the potential of a successful malicious software attack is greatly reduced.



Risk 2: Unauthorized Use of Passwords and/or System User Names

- Keeping your individual system user name and passwords **secure** is essential to maintaining the confidentiality, availability, and integrity of PHI
 - By keeping your user name and password confidential, you help ensure that e-PHI will be maintained correctly
 - Unauthorized use of individual user names compromises e-PHI and defeats the audit trails designed to monitor e-PHI use
- User names for terminated personnel will be disabled immediately



Never Share User Names or Passwords

- Sharing user names and passwords defeats the authorization procedures that have been put in place to control access to e-PHI based on a user's job responsibilities
- **You are responsible for all actions taken with your names**



Never Leave A Written Clue

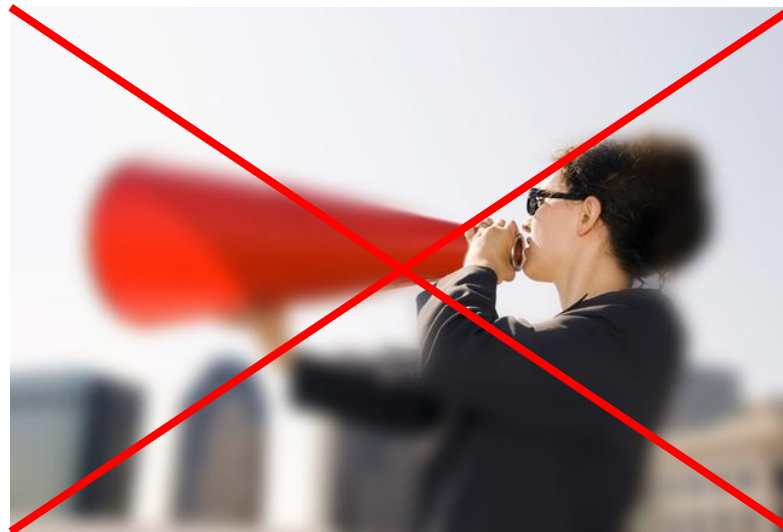
Your responsibilities

- Do not leave information at your workstation, laptop, or desk that could divulge what your system user names and passwords are
 - Never leave any written record of your system user names and passwords near your desk or workstation
- If you have to write them down, keep a record of passwords and system-user names in a secure location **away from your desk** and/or workstation
 - Never keep a record of your system-user names or passwords in luggage or laptop bags if they are going to be out of your immediate control

Passwords and User Names

Your responsibilities

- Never use another employee's user name and password
- Never ask another employee to reveal his/her personal user name and password
- **You are responsible for controlling your password maintenance!**



Quiz: Test Yourself

Question:

In case of emergency, it is a good practice to hide a copy of your user name and password under your workstation keyboard at your desk.

Is this true or false?



Quiz: Answer

The correct answer is false.

You should not leave information at your workstation, laptop or desk that could divulge your system user name and password because it provides easy access to unauthorized persons. If you must keep a record of this information, store it in a secure location away from your desk and/or workstation. Never keep a record of your system user name or password in luggage or laptop bags.



Risk 3: Weak or Ineffective Passwords

- Maintaining secure and strong passwords for systems and files is an essential element in achieving competent security for e-PHI
 - Passwords are your first line of defense for protecting the confidentiality and integrity of systems and files
 - Secure passwords are an essential safeguard against unauthorized use of your system user name or unauthorized access to your files
- To be effective, passwords must be:
 - Private and
 - Difficult to discover

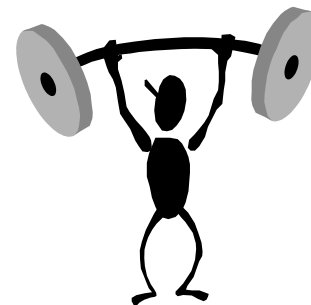


What Makes a Password STRONG?

- It cannot easily be found out
 - 12345, abcde, your name, birthday, or name of your child are ***not*** strong passwords!
- It contains more than 6 characters
- It contains a random combination of numbers and alphabetic characters
 - G258V74Z is a good example of a strong password

Tips for **STRONG** Passwords

- Avoid proper names or personal initials
- Avoid real words contained in either English or foreign language dictionaries
- Avoid personal dates of significance, like birth dates or anniversaries
- Never use a repeating pattern of letters and/or numbers
- Never repeat the corresponding user name as part of the password
- Use a combination of numbers and alphabetic characters, for example: **A9HZ37YT**



Quiz

Question:

Which of the following is a characteristic of a strong password?

Choose your answer:

- a) Contains the employee's date of birth
- b) An easy-to-remember word out of the dictionary
- c) A sequential string of either letters or numbers
- d) A random combination of numbers and alphabetic characters



Quiz Answer

The correct answer is (d).

Robust passwords consist of a random combination of numbers and alphabetic characters. Passwords comprised of repeating numbers, personal information (e.g., birth date), or common words may be easily guessed.



Steps to Further Safeguard e-PHI

- Take special care to protect portable media like laptops, Blackberries, and computer diskettes:
 - Password-protect the device to prevent access by unauthorized users
 - Keep these items in your personal possession when in public places
 - Do not check them with your luggage when traveling (e.g., on planes, trains, etc.)
 - Keep them in a locked suitcase or safe when in hotels
 - Exit all programs when the device is not in use



Steps to Further Safeguard ePHI

- Store all files containing e-PHI on network drives (rather than on local drives) to ensure the data is routinely backed up. Limit access to the network directory to e-PHI users
- Include e-PHI in attachments to emails, rather than in the text of the message itself. Password-protected or encrypt the attachment as warranted



Quiz

Question:

I don't need to implement password-protected access to my laptop.

Is this true or false?



Quiz Answer

The correct answer is false.

Access to data on portable media devices, such as laptops and Blackberries, must be password-protected at a minimum to prevent unauthorized users from gaining access to systems containing e-PHI.





HIPAA Privacy and Security Training

Breach notice rules

HIPAA Privacy and Security Rules – Breach notice rules

Breach notice obligations

- Effective 2009, a breach of PHI or ePHI not secured pursuant to prescribed “safe-harbor” standards (difficult to meet) require covered entities to:
 - Within 60 days, notify individuals whose PHI/ePHI is at risk because it was improperly disclosed or accessed
 - Notify the US Department of Health and Human Services of the breach
 - If breach affects 500 or more individuals in a jurisdiction, also notify the media
- Not every unauthorized access or disclosure will require a breach notice
 - Case-by-case evaluation required to see if breach notice rules are applicable

Safe harbor standards for encryption and destruction

At present, most employers have difficulty meeting the “safe harbor” rules for encryption and destruction that would relieve them of the breach notice obligations

Case-by-case evaluation required

Employer must evaluate, case-by-case, whether a specific breach requires notice

HIPAA Privacy and Security Rules

Breach notice responsibilities

- If you are aware of a breach of PHI or ePHI, contact the CSU HIPAA Privacy Official immediately
- Remember: HIPAA complaint and sanction policies apply to breach duties



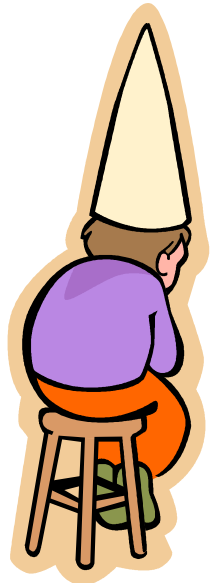


HIPAA Privacy and Security Training Sanction Policy

HIPAA Privacy and Security

CSU workforce sanctions

- CSU is committed to protecting the PHI and ePHI in our control and that we maintain on behalf of our health plans; we will enforce disciplinary sanctions on those employees who violate the procedures in the HIPAA Privacy and/or Security policies and procedures
- Based on the facts and circumstances of a particular violation, sanctions may range from oral warnings to termination of employment
- If you observe non-compliant behavior or practice on the part of another CSU employee or vendor, you should report it to the CSU HIPAA Privacy Official
- CSU maintains written Privacy and Security policies and procedures for safeguarding PHI and e-PHI as outlined in this training—and you are responsible for complying with these procedures



HIPAA compliance is **EVERYONE'S** responsibility!

Congratulations!

- You have completed the HIPAA Privacy and Security training course
- Thank you for participating in this required training



MERCER



MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

CSU BENEFITS OFFICERS

HR 2011-07
ATTACHMENT G

Tina Williams
Benefits Officer
CSU, BAKERSFIELD
9001 Stockdale Highway
Bakersfield, CA 93311-1099
(661) 654-3205
(661) 654-2299 (Fax)
twilliams@csubak.edu

Maurice L. Bryan
Director of Employment Practices/Dispute Resolution
CSU, CHICO
400 West First Street
Chico, CA 95929-0010
(530) 898-6771
(530) 898-5120 (Fax)
mlbryan@csuchico.edu

Juanita Aguilar
Benefits Manager
FRESNO STATE UNIVERSITY
5150 North Maple Ave., M/S #41
Fresno, CA 93740-0113
(559) 278-5336
(559) 278-4275 (Fax)
jaguilar@csufresno.edu

Karen Reynolds
Benefits Programs Specialist
CSU, EAST BAY
25800 Carlos Bee Blvd.
Hayward, CA 94542
(510) 885-2265
(510) 885-2951 (Fax)
karen.reynolds@csueastbay.edu

Felice Sparks
Benefits Manager
CSU, LONG BEACH
1250 Bellflower Blvd.
Long Beach, CA 90840
(562) 985-8266
(562) 985-4878 (Fax)
fsparks@csulb.edu

Angela Morgan
Benefits Coordinator and Training Officer
MARITIME ACADEMY
P. O. Box 1392
Vallejo, CA 94590
(707) 654-1137
(707) 654-1141 (Fax)
AMorgan@sum.edu

Diana Enos
Benefits and Compensation Manager
CSU, CHANNEL ISLANDS
One University Drive
Camarillo, CA 93012
(805) 437-8426
(805) 437-8491 (Fax)
diana.enos@csuci.edu

Brian Cummins
Benefits Manager
CSU, DOMINGUEZ HILLS
1000 East Victoria Street
Carson, CA 90747
(310) 243-3005
(310) 516-3595 (Fax)
bcummins@csudh.edu

Denise Johnson
Director, HR Operations
CSU, FULLERTON
2600 E. Nutwood Ave., #700.
Fullerton, CA 92834-9480
(657) 278-2425
(657) 278-7188 (Fax)
djohnson@fullerton.edu

Cindy Darnall Stevens
Benefits Administrator
HUMBOLDT STATE UNIVERSITY
One Harpst Street
Arcata, CA 95521-8299
(707) 826-5171
(707) 826-3625 (Fax)
darnallc@humboldt.edu

Deborah Williams
Mgr., Compensation, Classification & Benefits
CSU, LOS ANGELES
5151 State University Drive
Los Angeles, CA 90032
(323) 343-3676
(323) 343-3662 (Fax)
dwillia@cslanet.calstatela.edu

Yvonne Chambers
Lead Benefits and Workers' Compensation Analyst
CSU, MONTEREY BAY
100 Campus Center
Seaside, CA 93955
(831) 582-3387
(831) 582-3614 (Fax)
YChambers@sumb.edu

CSU BENEFITS OFFICERS

Laurie Gold-Brubaker
Benefits Manager
CSU, NORTHRIDGE
18111 Nordhoff Street
Northridge, CA 91330
(818) 677-3809
(818) 677-7200 (Fax)
laurie.gold-brubaker@csun.edu

Mary Ford
Benefits Manager
CSU, SACRAMENTO
6000 J Street, SH 253
Sacramento, CA 95819
(916) 278-6213
(916) 278-7331 (Fax)
fordmr@csus.edu

Jennifer Acfalle
Senior Benefits Analyst
SAN DIEGO STATE UNIVERSITY
5500 Campanile Drive
San Diego, CA 92182-1625
(619) 594-1142
(619) 594-4013 (Fax)
jacfalle@mail.sdsu.edu

Rick Casillo
Associate Director, Employee Support and Service
SAN JOSE STATE UNIVERSITY
One Washington Square
San Jose, CA 95192
(408) 924-2272
(408) 924-2161 (Fax)
rick.casillo@sjsu.edu

Yasuko Shirakawa
Benefits Coordinator
CSU, SAN MARCOS
333 South Twin Oaks Valley Road
San Marcos, CA 92096-0001
(760) 750-4425
(760) 750-3141 (Fax)
yasukos@csusm.edu

Kelly Mode
Benefits & Workers Comp Administrator
CSU, STANISLAUS
One University Circle
Turlock, CA 95382
(209) 667-3353
(209) 664-7011 (Fax)
kmode@stan.csustan.edu

Ghazala Khan
Benefits Analyst
CALPOLY, POMONA
3801 West Temple Ave., Bldg. 98
Pomona, CA 91768
(909) 869-3735
(909) 869-4868 (Fax)
gkkhan@csupomona.edu

Lillian Hernandez
Manager, Employee Benefits & Workers Comp
CSU, SAN BERNARDINO
5500 University Parkway
San Bernardino, CA 92407
(909) 537-3102
(909) 537-7019 (Fax)
lillianh@csusb.edu

Wanda M. Humphrey
Interim Payroll and Benefits Manager
SAN FRANCISCO STATE UNIVERSITY
1600 Holloway Ave., ADM-252
San Francisco, CA 94132
(415) 338-2628
(415) 338-0521 (Fax)
Maxine@sfsu.edu

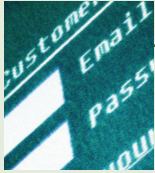
Kathy Constantine
Benefits Officer
CAL POLY, SAN LUIS OBISPO
One Grand Ave.
San Luis Obispo, CA 93407
(805) 756-6571
(805) 756-5483 (Fax)
kconstan@calpoly.edu

Susan Zito
Manager, Payroll and Benefits
SONOMA STATE UNIVERSITY
1801 East Cotati Ave.
Rohnert, CA 94928
(707) 664-2178
(707) 664-2024 (Fax)
susan.zito@sonoma.edu

Vivian Dea
Benefits Officer
CSU, CHANCELLOR'S OFFICE
401 Golden Shore, 2nd Floor
Long Beach, CA 90802
(562) 951-4078
(562) 951-4899 (Fax)
vdea@calstate.edu

Information Security Management

Top Ten List of Good Security Practices



1. Use complex passwords that cannot be easily guessed.

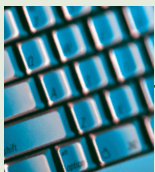
- Do not share your passwords.
- Avoid writing your passwords down.
- Characteristics of good, complex passwords:
 - At least 8 characters in length;
 - Contain a mixture of upper and lower case letters, numbers, and symbols;
 - Difficult to guess (e.g., do not include real words or personal information like user name, account numbers, names of family members, places, pets, birthdays, hobbies, etc.); and
 - Easy to remember (so you don't have to write them down).
- Examples of complex passwords:
 - 4>or<Zero\$
 - Oh2SURV!e#

For more information on password policy, visit http://intranet.calstate.edu/technology_services/desktop_services/policies/passwords.asp.



2. Secure your working area and computing equipment before leaving them unattended.

- Use laptop lockdown cables to secure your laptop.
- Store PDAs, purses, wallets, or anything valuable in a locked cabinet to prevent theft.
- Put away sensitive documents and other materials in a locked cabinet before you leave your work area or when you leave at the end of the workday.
- Never share your access code, card, or keys.



3. Shut down, lock, log off of, or put your computer to sleep before leaving it unattended.

- On a PC, use <ctrl> <alt> or <Windows> <L>.
- Use Apple menu or <option> <Apple> <eject> on a Mac.



4. Be cautious when using the Internet.

- Do not provide personal or sensitive information in response to an unsolicited request whether it is over the phone, over the Internet, or from an e-mail message.
- Be aware of where you are going before clicking on a Web link. When in doubt, instead of clicking on an unknown or solicited link, look up the website on your own and go there independently.
- Do not send or open files sent via instant messaging (IM). IM tends to bypass antivirus scanning, making it easier for these files to infect your computer.
- Do not use peer-to-peer file sharing software.
- Do not save your user name and passwords to websites or accounts. Instead, type them in every time you log in.
- For home networks, use a personal firewall.



5. Practice safe e-mailing.

- Do not open an e-mail attachment if it is from someone you do not know.
- Be cautious with opening an e-mail attachment even if it is from someone you know.
- Do not click on website addresses in e-mails unless you really know what you are opening.
- Delete spam and suspicious e-mails; do not open, forward, or reply to them.
- Use courtesy when sending, replying, and forwarding jokes of poor taste in nature.
- Avoid participating in chain letter e-mails.



6. Make sure your computer is protected with antivirus and all necessary security “patches” and updates, and that you know what you need to do, if anything, to keep them current.

- Do not attempt to disable your anti-virus settings.
- Ensure your home computer is protected as well.



7. Do not keep private information or your only copy of critical data, projects, etc., on portable devices (such as laptop computers, home computers, CDs/floppy disks, memory sticks, PDAs, data phones, etc.) unless they are properly protected. These items are extra-vulnerable to theft or loss.

- Do not store CO-related or any CSU-related confidential data on your personal/home computers.
- If you absolutely need to store confidential or personal data on portable devices, use sufficient protection to secure the data. Contact ISM for further assistance.



8. Do not install or download unknown or suspicious programs to your computer.

- These can harbor behind-the-scenes computer viruses or open a “back door” giving others access to your computer without your knowledge.



9. Make sure to make copies of data you are not willing to lose—and store the copies in a secure manner.



10. When in doubt, ask for help.

- Contact ISM
 - infosec@calstate.edu
- Contact Service Desk
 - itservicecenter@calstate.edu
 - 562-346-2456, 7 days a week, 24 hours a day (holidays included)

References

- <http://staysafeonline.org>
- <http://www.scambusters.org>