California State University

HIPAA Privacy Summary Manual

As prepared by

MERCER
Human Resource Consulting

The HIPAA Privacy Summary 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). Any reproduction or other use for commercial or other purposes is not permitted without the express written permission of Mercer Human Resource Consulting (Mercer).

Table of Contents

1. Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) 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 Summary 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 Summary 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 9.01 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 Summary Manual is designed to be the Policies and Procedures for the health plan(s) in Section 9.01, referred to throughout as the "Plan". Because each plan is sponsored by CSU, they collectively comprise an "organized health care arrangement" and the Summary Manual represents the Policies and Procedures for each plan. The HIPAA Privacy Rule and this Summary 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.

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 Summary Manual consists of nine (9) sections.

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

Section 2 defines key terms that are used in this Summary Manual. The defined terms are capitalized throughout the Summary 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 key resources related to the implementation of this Summary Manual. It includes the name of the Privacy Official responsible for the development, coordination, implementation, and management of the Summary Manual. In addition, it includes the Forms that CSU will be using to meet the privacy requirements, along with instructions for using those forms.

The Summary Manual 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 9.

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 8.04.

Amendment: A change or modification.

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 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 8.03.

Campus Privacy Contact: The persons or offices specified in Section 9.03 who are responsible for responding to Participants exercising their rights described in Section 6 and for other duties specified in Section 9.03.

Confidential Communication: An alternative means or alternative locations to communicate PHI to the Participant.

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.

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

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.

Marketing: 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.

In addition, marketing includes an arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Minimum Necessary*:* To the extent practical, individually identifiable health information should be disclosed only to the extent needed to support the purpose of disclosure. Covered Entities are expected to make a reasonable effort to limit use, disclosure of, and requests for PHI to the *Minimum Necessary*. HIPAA requires Covered Entities to make their own assessment of what health information is reasonably necessary.

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, as codified in this Summary 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

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.

Enrollment information received by CSU directly from employees is not PHI. However, individual enrollment information received from the health insurance carriers, HMOs, external EAP vendors and HCRA claims administrator is PHI. In addition, the following are examples of PHI at CSU:

- Formal HCRA claim appeals (to be handled by the Systemwide Human Resources Administration benefits staff only); and
- Information received from the health insurance carriers, HMOs, external EAPs or HCRA claims administrator (after obtaining the Participant's Authorization) regarding customer service and claim advocacy for a Participant.

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	• 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)	• 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 Minimum Necessary (e.g., refrain from forwarding strings of e-mail messages containing PHI. Instead, prepare a new message, with only the Minimum Necessary information) • 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
	• 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	• 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	• Limit the content of PHI in conversations (e.g., with vendors and other staff) to the Minimum Necessary. • Verify the identity of individuals on the phone (see Section 4.03). • 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.

*** Please notify the Privacy Official immediately if you receive any such request.**

5. 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 8.03).

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
- If requested by a Health Care Provider for Treatment;
- If needed for Payment activities such as claims, appeals and bill collection;
- 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. You should immediately contact the Privacy Official if you 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.

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 Summary 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)

5.02 Enrollment and Disenrollment 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) to CSU (or its agents) in the following circumstances:

PHI disclosed	Employer uses of PHI
Enrollment and disenrollment information	• 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.

The enrollment and disenrollment 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 Summary Manual.

5.03 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.

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. However, 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's Authorization.

Customer service procedures governing disclosures and requests made on a routine and recurring basis are described in the following chart.

a. Customer Service

Certain CSU staff assist 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.	
CSU staff permitted access to PHI	• Campus benefits staff • Systemwide Human Resources Administration benefits staff • Chancellor's Office staff involved in benefit administration
Parties to whom disclosures are permitted	• 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.) and Insurers involved in benefit determinations.

	• Business Associates (e.g., external EAP vendors, HCRA claims administrator, health care benefits consultants, etc.) and Insurers assisting with review and analysis of benefit determinations.
Categories of PHI	• All PHI relevant to the claim.
Protocols for meeting Minimum Necessary requirement	• CSU staff will disclose only 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	• Paper records will be maintained in a separate file from employment records. • Information will be protected using the procedures in Section 4.02.
Retention/ Destruction	• PHI will be maintained for at least 6 years after creation and will then be destroyed.

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 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 8.04.

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.

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.

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.

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 chart below.

If you receive any such disclosure requests, you must immediately contact the Privacy Official.

Purpose for disclosure	Permissible disclosures of PHI
Workers' compensation	• 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	• 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	• 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	• Includes disclosures of PHI to government authorities, including social services or protected services agencies

Purpose for disclosure	Permissible disclosures of PHI
violence	authorized by law to receive reports of abuse, neglect, or 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	• 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	• 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	• 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	• Includes disclosures of PHI to organ procurement organizations or other entities to facilitate cadaveric organ, eye, or tissue donation and transplantation.
Research purposes	• 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	• 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.

Purpose for disclosure	Permissible disclosures of PHI
Specialized government functions	• Includes disclosures of PHI of individuals who are Armed Forces personnel or foreign military personnel under appropriate military command authority. • 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	• 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 Summary 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. 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;
- Social Security number;
- Specific dates such as dates of birth and death, and admission/discharge dates. *The Plan can use the year of the event, except for the birth years of persons over age eighty-nine (89)*
- Telephone numbers;
- Fax numbers;
- E-mail addresses;
- Medical record numbers;
- Geographic identifiers smaller than a state, including street address, city, county, precinct, and zip code. *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;*
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers (serial numbers or license plate
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers (e.g., finger, iris, or voice prints);
- Full-face photographic and any comparable images; and
- Any other unique

• Health plan beneficiary number;	numbers);	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 Summary 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.

6. Individual Rights

6.01 Overview

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 9.07(a) for request Form);
- Request the Amendment of their PHI in a Designated Record Set; (see Section 9.07(b) for request Form);
- Request restriction of the use and disclosure of their PHI;(see Section 9.07(c) for request Form);
- Request the use of alternative means or alternative locations for receiving communications of their PHI (see Section 9.07(d) for request Form); and
- Request an accounting of PHI disclosures (see Section 9.07(e) for request Form).

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. 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 coverages 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, please have the Participant fill out the applicable Form from Section 9.07 and send that Form immediately to the Privacy Official. The Privacy Official will handle the request.

7. Risk Management Activities

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 Summary Manual (including limiting the use, disclosure of PHI as required under Section 5). The Campus Privacy Contacts will coordinate the training for each CSU campus. 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, which are included in this Summary Manual, are to be covered in the training:

Training topic
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
How to respond when a violation of the HIPAA Privacy Rule or the Plan's Policies and/or Procedures occurs

Training topic
The possible sanctions if a workforce member violates the HIPAA Privacy Rule or the Plan's Policies and Procedures

The Campus Privacy Contact should review the contents of this Summary Manual with employees who will have access to PHI. In addition, Campus Privacy Contact should familiarize employees with the HIPAA materials and information contained on the CSU Employee Benefits Program web-site: http://www.calstate.edu/benefits/healthcare.shtml. If a campus lacks a Campus Privacy Contact to conduct the training, please contact the Privacy Official.

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	CSU specifics	Done
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		

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

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.

7.05 Mitigation

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

a. Mitigation Steps

If CSU knows of harmful effects resulting from its own improper use or disclosure of PHI, CSU will consider a variety of steps, including:

- Investigating the facts and circumstances of the use or disclosure of PHI;
- Contacting the affected parties;
- Reviewing the PHI in question;
- Assisting the affected parties, and
- Contacting the workforce member(s) or the Business Associate(s) involved in the situation.

Each Campus Privacy Contact will conduct the mitigation activities for his or her campus and will notify the Privacy Official regarding the improper use and disclosure of PHI.

In addition, the Privacy Official and Campus Privacy Contact may apply sanctions (see Section 7.04) against workforce members who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule.

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 each Campus Privacy Contact will retain under this rule:

Documents
☐ Privacy Policies and Procedures (this Summary Manual)
☐ Authorizations
☐ Privacy Agreements for External EAPs
☐ Notices of Privacy Practices
☐ Documentation that training has been provided to employees

Key person identification
☐ Name of Privacy Official
☐ Name of Campus Privacy Contact

Other materials relating to particular actions by the Plan
☐ Documentation of sanctions applied to employees for not complying with the HIPAA Privacy Rule, if any

8. Required Legal Documents

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 Privacy Agreement/Business Associate Agreement describes the permitted uses and disclosures of PHI by the external EAPs.

- 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 8.04).

8.02 Privacy Notice

CSU will provide a Multi Benefit Plan Privacy Notice in Section 9.06 to satisfy the notice obligation for the HCRA and external EAPs. Each health insurance carrier 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 9.06 to new hires. In addition, CSU will provide the Multi Benefit Plan Privacy Notice to Participants upon request.

a. Identifying the Recipients

Campus Privacy Contacts will provide the Privacy Notice (see Section 9.06) to Participants who are covered under the HCRA and external EAP plans, no later than April 14, 2004. Campus Privacy Contacts 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, Campus Privacy Contacts will provide the Privacy Notice to all external EAPs and to workforce members who perform Plan functions, during their initial training and when necessary thereafter.

b. Distributing the Notice

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

Campus Privacy Contacts also may provide the Notice by e-mail, if the Participant has agreed to electronic notice and the agreement has not been withdrawn. Campus Privacy Contacts 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), Campus Privacy Contacts

will provide the revised Privacy Notice to Participants covered under the HCRA and external EAP plans 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, Campus Privacy Contacts 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, Campus Privacy Contacts 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.

8.03 Privacy/Business Associate Agreements

The HIPAA Privacy Rule requires each Business Associate of the Plan to enter into a written contract (a Privacy/Business Associate Agreement) with the Plan before the Plan can disclose PHI to it, except as indicated below. The Business Associate can use and disclose PHI only for the purposes provided in the Business Associate Agreement. A Business Associate not yet required to enter into a Privacy/Business Associate Agreement must still comply with the HIPAA Privacy Rule.

a. Identifying Business Associates and Signing Agreements

CSU will determine which service providers are Business Associates. At present, CSU has determined that the external EAP vendors, the HCRA claims administrator, and its benefits consultants, and its outside counsel, are business associates. The log of Privacy/Business Associate Agreements is at Section 9.04.

The Plan will require each Business Associate to sign a Privacy/Business Associate Agreement (see Section 9.04) or a contract that contains the required terms, as determined by the Privacy Official. Campus Privacy Contacts will be responsible for obtaining a Privacy Agreement from the external EAPs. See section 9.04 for the model Privacy Agreement.

b. Documenting Privacy Agreements with the External EAP.

All Privacy Agreements will be retained for a period of at least six (6) years from the date they were last in effect.

8.04 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 9.07(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 9.03). 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.

9. Key Resources and Forms

9.01 Covered Plans

CSU sponsors the following group health plan(s):

- CalPERS Health Care Providers (medical and prescription drug coverage)
  - Blue Shield HMO
  - Kaiser
  - PERSCare
  - PERS Choice
  - Peace Officer Research Association of California (PORAC)
  - Western Health Associates (WHA)
- Delta Dental (dental coverage)
- PMI Delta Care DMO
- Blue Shield (vision)
- Health Care Reimbursement Account (HCRA) Plan
- External EAPs that provide counseling services
  - PacifiCare Behavioral Health (Bakersfield, California Maritime Academy, Chancellor's Office, Channel Islands, Hayward, San Luis Obispo)
  - Integrated Insights (Dominguez Hills, San Diego, San Marcos)
  - Humboldt Family Services (Humboldt)
  - Community Action EAP (Los Angeles)
  - Dorris and Associates (Fullerton)
  - Magellan Behavioral Health (Monterey Bay)
  - Concern EAP (San Jose)
  - Employee Development Services (Sonoma)
  - Managed Health Network (Stanislaus)

9.02 Privacy Official

a. Privacy Official Designation

The following person is designated as the Privacy Official:

Name: Beth Ryan

Title: Senior Manager, Human Resources Relations & Projects

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

Phone: (562) 951-4420

Fax: (562) 951-4954

Email: bryan@calstate.edu

In the absence of the above named Privacy Official, the following person is designated as the Privacy Official:

Name: Pamela Chapin

Title: Senior Manager, Benefits and Salary Programs

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

Phone: (562) 951-4414

Fax: (562) 951-4954

Email: pchapin@calstate.edu

9.03 Campus Privacy 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.
- Obtain Privacy Agreements with the external EAPs.
- 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

9.04 Privacy/Business Associate Agreements

a. Model Privacy/Business Associate Agreement

Directions to CSU for Using Model Privacy Agreement

General Comments. The Privacy Agreement is specifically for the external EAP plans. If the Campus Privacy Contact identifies other business associates, he or she should contact the Privacy Official for the correct form of agreement. The Privacy Agreement is designed to be a addendum to existing contracts between CSU and its external EAPs. It should be modified if it will be used as a stand-alone contract (i.e., there is no existing contract), or for insertion into the body of a contract.

Select Instructions:

Section 3.0(b). This section is optional. Most vendors will likely request the authority to engage in the specific uses and disclosures discussed therein.

Section 6.0(a). External EAP plans, CSU has until April 14, 2004.

Section 7.0(f). Conform this section to the existing contract with this vendor unless that contract does not specify the law of which state will govern the contract.

Section 7.0(g). Modify this section if the existing contract does not include any provision regarding indemnification or performance guarantees, or if application of those provisions requires additional statements in this section.

HIPAA PRIVACY AGREEMENT

This Agreement is entered into this _____ day of _____, 2004, between the California State University ("Plan Sponsor"), acting on behalf of its Employee Assistance Plans (collectively, the "Plan"), and _____ ("Vendor"). The Agreement is incorporated into the Agreement for Employee Assistance Program Services between Plan Sponsor and Vendor**,** effective _____ (the "Service Contract"). The Plan and Vendor intend for this Agreement to satisfy the Business Associate contract requirements in the regulations at 45 CFR 164.502(e) and 164.504(e), issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), if those regulations are applicable to the Plan in regards to this Vendor.

1.0 Definitions

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 CFR 160.103 and 164.501. Notwithstanding the above, "Covered Entity" shall mean the Plan (as defined above); "Individual" shall have the same meaning as the term "individual" in 45 CFR 164.501 (and effective April 21, 2003, 45 CFR 160.103) and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g); "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his designee; and "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.

2.0 Obligations and Activities of Vendor

(a) Vendor 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.

(b) Vendor agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

(c) Vendor agrees to mitigate, to the extent practicable, any harmful effect that is known to Vendor of a use or disclosure of Protected Health Information by Vendor in violation of the requirements of this Agreement.

(d) Vendor agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

(e) Vendor agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Vendor on behalf of, Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Vendor with respect to such information.

(f) Vendor agrees to provide access, at the request of Covered Entity, to Protected Health Information for the sole purpose of auditing health plan claims by an auditor, selected by Plan Sponsor, and for resolving any issues that may arise as a result of such an audit.

(g) Vendor 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.

(h) Vendor 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.

(i) Vendor 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 Vendor 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.

(j) Vendor 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.

(k) Vendor 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.

(l) Vendor 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 no later than October 16, 2003. Vendor further agrees to ensure that any agent, including a subcontractor, that conducts standard transactions on its behalf will comply with the EDI Standards.

(m) Vendor 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).

3.0 Permitted or Required Uses and Disclosures by Vendor

(a) General Use and Disclosure. Except as otherwise limited in this Agreement, Vendor may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Service 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.

(b) Additional use and disclosure.

(i) Except as otherwise limited in this Agreement, Vendor may use Protected Health Information for the proper management and administration of the Vendor or to carry out the legal responsibilities of the Vendor.

(ii) Except as otherwise limited in this Agreement, Vendor may disclose Protected Health Information for the proper management and administration of the Vendor, provided that such disclosures are required by law, or Vendor 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 Vendor 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, Vendor 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) Vendor 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 Obligations of Covered Entity to Inform Vendor of Covered Entity's Privacy Practices, and any Authorization or Restrictions.

(a) Covered Entity shall provide Vendor 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 Vendor 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 Vendor's uses or disclosures of Protected Health Information.

(c) Covered Entity shall notify Vendor 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 Vendor's uses or disclosures of Protected Health Information.

5.0 Permissible Requests by Covered Entity.

Covered Entity shall not request Vendor 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 April 14, 2004**,** and shall terminate when all of the Protected Health Information provided by Covered Entity to Vendor, or created or received by Vendor 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.* Without limiting the termination rights of the parties pursuant to the Service Contract, and upon Covered Entity's knowledge of a material breach by Vendor of a provision under this Agreement, Covered Entity shall provide an opportunity for Vendor to cure the breach or end the violation and terminate the Service Contract if Vendor does not cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate the Service Contract if Vendor 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.

(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 Vendor as its custodian for the safe keeping of any record-containing Protected Health Information that Vendor may determine it is appropriate to retain. Notwithstanding the expiration or termination of the Service Contract, Vendor 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) *Effect on Covered Entity Status*. This Agreement shall in no way effect or limit Vendor's obligations and duties under HIPAA as a covered entity under HIPAA. Vendor shall be fully responsible for compliance with all the requirements of HIPAA in its capacity as a covered entity under HIPAA in providing services and benefits to the Plan.

(b) *Regulatory References.* A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended, and for which compliance is required.

(c) *Amendment.* The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and HIPAA.

(d) *Survival.* The respective rights and obligations of Vendor under Section 6.0 of this Agreement shall survive the termination of this Agreement.

(e) *Interpretation.* Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

(f) *No third party beneficiary.* Nothing expressed or implied in this Agreement or in the Service 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.

(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 Rules or other applicable federal law.

(h) *Indemnification and performance guarantees*. The indemnification and performance guarantee provisions contained in the Service Contract shall also apply to this Agreement.

The Employee Assistance Plans

By: The California State University
By: _____
Name: _____

Their: Plan Sponsor

_____**[NAME OF EXTERNAL EAP VENDOR]**

By: _____
Name: _____
Its: _____

b. Log of Business Associate Agreements

Vendor name	Agreement date	Expiration date	Storage location	Description of agreement (including Plan names)
PacifiCare Behavioral Health				EAP vendor (5 campuses and Chancellor's Office)
Integrated Insights				EAP vendor (3 campuses)
Humboldt Family Services				EAP vendor (1 campus)
Community Action EAP				EAP vendor (1 campus)
Dorris and Associates				EAP vendor (1 campus)
Magellan Behavioral Health				EAP vendor (1 campus)
Concern EAP				EAP vendor (1 campus)
Employment Development Services				EAP vendor (1 campus)
Managed Health Network				EAP vendor (1 campus)

9.05 Insurers

The following is a list of the Plan(s) Insurers:

Insurer	Policy identifying information
CalPERS Health Care Providers	Medical / Rx
Delta Dental	Dental
PMI Delta Care DMO	Dental
Blue Shield Life	Vision

9.06 Notice of Privacy Practices

Instructions for Privacy Notice

The Privacy Notice included in Section 9.06 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.

CSU MULTI BENEFIT PLAN PRIVACY NOTICE

[ATTACHED]

9.07 Participant Forms

The following forms are included in this Section:

9.07 (a) Request for Access to Inspect and Copy

9.07 (b) Request to Amend

9.07 (c) Requests for Restricted Use

9.07 (d) Request for Confidential Communications

9.07 (e) Request for Accounting of Non-Routine Disclosures

9.07 (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. **Determination of Request.** Upon receipt of this Form with Part I properly completed, the Campus Privacy Contact will immediately forward it to the Privacy Official.

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.

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 ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	**3a. Your Relationship to Person in Box 2** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **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 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 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/privacyhowtofile.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. **Determination of Request.** Upon receipt of this Form with Part I properly completed, the Campus Privacy Contact will immediately forward it to the Privacy Official.

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 ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	**3a. Your Relationship to Person in Box 2** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **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 Heath 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. **Determination of Requests for Restricted Use of PHI.** When Part I, Section A has been completed, the Privacy Contact will immediately forward the form to the Privacy Official.

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 ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	**3a. Your Relationship to Person in Box 2** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **Other (please describe relationship):**
4. Mailing Address for Records	**4a. City, State, Zip Code**

Section A: Request to Restrict Use and Disclosure of Personal Heath 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 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 Heath 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. **Determination of Request**. Upon receipt of this Form with Part I properly completed, the Campus Privacy Contact will immediately forward it to the Privacy Official.

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 ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	**3a. Your Relationship to Person in Box 2** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **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 an external EAP, 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. **Determination of Request**. Upon receipt of the Form with Part I properly completed, the Campus Privacy Contact will immediately forward it to the Privacy Official.

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 ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name	**3a. Your Relationship to Person in Box 2** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **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-routines 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 external 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 at 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 CSU's health plans (including the HCRA Plan), Privacy Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form, the 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 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, Insurers 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 addition 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.

HIPAA AUTHORIZATION FORM

[ATTACHED]