

SAN DIEGO COUNTY EMPLOYEES RETIREMENT ASSOCIATION
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY POLICY
AND PRIVACY CERTIFICATION

I. PURPOSE

To affirm and document the San Diego County Employees Retirement Association Retiree Health Program's (the "Health Plan's") compliance with the privacy rules set forth in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and its implementing regulations (45 CFR Parts 160 and 164). Additionally, this certifies that the Plan Sponsor, the San Diego County Employees Retirement Association ("SDCERA"), has agreed to certain restrictions on its use of Protected Health Information (as defined below), as specified in Section III, below.

The Health Plan is a fully insured group health plan sponsored by SDCERA. The Health Plan provides benefits solely through several insurance contracts with health insurance issuers or health maintenance organizations (collectively, the "Insurers"). The Health Plan and SDCERA intend to comply with the requirements of 45 CFR § 164.530(k), so that the Health Plan is not subject to most of HIPAA's privacy and security requirements. The Insurers, however, are subject to HIPAA's privacy and security rules as covered entities. This Policy is intended to comply with the requirements of HIPAA, and may be changed or terminated at any time. The Health Plan is not subject to the Employee Retirement Income Security Act of 1974 ("ERISA"). The Plan shall be construed and enforced according to the laws of the State of California.

II. POLICY

A. No Access to Protected Health Information Except for Summary Health Information for Limited Purposes and Enrollment/Disenrollment Information

Neither the Health Plan nor SDCERA (or any member of SDCERA's workforce) shall create or receive protected health information ("PHI"), as defined by 45 CFR §160.103, except for the following:

1. "Summary health information," as defined by HIPAA's privacy rules (45 CFR § 164.504(a)), for purposes of (a) obtaining premium bids, or (b) modifying, amending, or terminating the Health Plan;
2. Enrollment and disenrollment information concerning the Health Plan which does not include any substantial clinical information; or
3. PHI disclosed to the Health Plan and/or SDCERA under a signed authorization that meets the requirements of the HIPAA privacy rules.

B. Insurers for Health Plan Will Provide Privacy Notices

1. The Insurers for the Health Plan will provide the Notice of Privacy Practices required by the HIPAA regulation (45 CFR § 164.520) and will satisfy the other requirements under HIPAA's privacy rules related to Notice of Privacy Practices. The Notice of Privacy

Practices, among other things, will notify Health Plan participants of the potential disclosure of the summary health information and enrollment and disenrollment information to the Plan and SDCERA.

C. Breach Notification Requirements

The Health Plan shall comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") and its implementing regulations to provide notification to affected individuals, the Department of Health and Human Services ("HHS"), and the media, when required, if the Health Plan or one of its business associates discovers a breach of unsecured PHI.

D. No Intimidating or Retaliatory Acts

The Health Plan shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual for:

1. Exercising his or her rights under the HIPAA rules;
2. Participating in any process provided for by the HIPAA rules, including the filing of a complaint with HHS;
3. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing provided for under the HIPAA rules; or
4. Opposing any act or practice that is prohibited by HIPAA, if such individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA regulations.

E. No Waiver of HIPAA Privacy Rights

The Plan shall not require an individual to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility for benefits.

F. Technical and Physical Safeguards and Firewall

SDCERA will establish on behalf of the Health Plan appropriate technical and physical safeguards to prevent PHI from being used or disclosed (intentionally or unintentionally) in violation of HIPAA's requirements. Technical safeguards of PHI include limiting access to PHI by creating computer firewalls and by prohibiting access by SDCERA employees to PHI held by the Insurers, except as permitted by law and under this Policy. To the extent any PHI is obtained by SDCERA, safeguards have been established so that only its workforce has access to PHI, and any such PHI is limited to the minimum amount necessary for Health Plan administrative functions.

G. Privacy Official and Security Official

SDCERA 's Chief Operating Officer is the Privacy Official and SDCERA's Director, Information Technologies is the Security Official for the Plan. The Privacy Official is responsible for the development and implementation of policies and procedures related to

privacy of Plan participants' PHI. The Security Official is responsible for the development and implementation of policies and procedures relating to the physical and technological security of PHI that is received, maintained, or transmitted in electronic form. The Privacy Official and the Security Official will also serve as the contact persons for participants who have questions, concerns, or complaints about the privacy or security of their PHI. The Privacy Official and the Security Official may be reached at (619) 515-6800.

H. Workforce and Workforce Training

The Plan's workforce will be trained and will receive ongoing training as necessary with regard to HIPAA's privacy and security requirements. As of January 1, 2011, the individuals within the following departments are considered to be the Health Plan's workforce for which HIPAA training is required: Member Services, Administrative Services, and Information Technology.

I. Mitigation of Inadvertent Disclosures of PHI

SDCERA and the Privacy and Security Officials shall mitigate, to the extent possible, any harmful effects that become known to them of a use or disclosure of a Plan participant's PHI in violation of HIPAA and this Policy, or of a security breach that involves electronic PHI.

J. Sanctions for Violations of Plan Privacy Policies

SDCERA employees who use or disclose PHI in violation of HIPAA and this Policy will be subject to disciplinary action, up to and including termination of employment.

K. Documentation and Recordkeeping

Any changes to this Policy shall be documented. The Health Plan's workforce (or the Insurers, as appropriate) shall document all actions (including authorizations, requests for information, disclosures, sanctions, security breaches and complaints) related to a Health Plan participant's PHI during the prior six years, and will, upon request, provide an accounting of disclosures that were made to third parties for purposes other than: (i) treatment; (ii) payment; or (iii) health care operations; or (iv) pursuant to a valid authorization signed by the Participant; or (v) a disclosure of a participant's PHI to the Participant him or herself. Additionally, the Plan (or the Insurers, as appropriate) must retain each participant's Designated Record Set for a period of six years from the later of the date on the record's creation or the date it was last in effect.

L. Business Associates

To the extent required by law, SDCERA will enter into business associate agreements with agents or subcontractors of the Health Plan to whom the Health Plan provides PHI. Business Associates must agree in writing to be subject to the same restrictions and conditions under HIPAA that apply to the Plan.

M. Other Matters

No third-party rights (including but not limited to rights of Health Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Health Plan reserves the right to amend or change this Policy and its internal procedures at any time (and

retroactively) without notice. This Policy does not address privacy or other requirements under state law or federal laws other than HIPAA.

III. HIPAA PRIVACY CERTIFICATION OF THE SAN DIEGO COUNTY EMPLOYEES RETIREMENT ASSOCIATION RETIREE HEALTH PROGRAM

SDCERA, in its capacity as sponsor of the San Diego County Employees Retirement Association Retiree Health Program (the "Health Plan"), a "group health plan," as defined 45 CFR §164.160, hereby certifies that it has reviewed the Health Plan's HIPAA Privacy Policy and certifies that as Plan Sponsor, it shall:

- Not use or further disclose Protected Health Information ("PHI"), as defined by 45 CFR §160.103, other than as permitted or required by the Health Plan or as required by law;
- Ensure that any agent, including a subcontractor, to whom it provides PHI received from the Health Plan agrees to the same restrictions and conditions that apply to SDCERA with respect to PHI;
- Not use or disclose the PHI for employment-related actions and decisions, or in connection with any other benefit or employee benefit plan sponsored by SDCERA;
- Report to the Health Plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
- Make available PHI to comply with HIPAA's right to access in accordance with 45 CFR §164.524;
- Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 CFR §164.526;
- Make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528;
- Make its internal practices, books, and records relating to the use and disclosure of PHI received from the Health Plan available to the Secretary of Health and Human Services for purposes of determining compliance by the Health Plan with HIPAA's privacy requirements;
- If feasible, return or destroy all PHI received from the Health Plan that SDCERA maintains in any form, and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, SDCERA shall limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
- Ensure that the adequate separation between Health Plan and SDCERA, as required by 45 CFR § 504(f)(2)(iii), is satisfied.

SAN DIEGO COUNTY EMPLOYEES RETIREMENT ASSOCIATION

By: _____

Date signed: _____

IV. EFFECTIVE DATE

This Policy and Certification is effective as of the date on which HIPAA's privacy rules first applied to the Health Plan, and shall continue in force except as modified in writing.

REVIEW

The Board will review this policy at least every three (3) years to ensure it remains relevant and appropriate.

HISTORY

January 6, 2011	Adopted, effective immediately
June 5, 2014	Reviewed, no changes