SAN DIEGO COUNTY EMPLOYEES RETIREMENT ASSOCIATION

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT SECURITY POLICY

I. PURPOSE

The San Diego County Employees Retirement Association Retiree Health Program (the "Health Plan") is a fully-insured group health plan sponsored by the San Diego County Employees Retirement Association ("SDCERA," or the "Plan Sponsor"). The Health Plan provides benefits solely through insurance contracts with health insurance issuers or health maintenance organizations (collectively, "Insurers"). Neither SDCERA nor any member of its workforce creates, receives, maintains, or transmits electronic Protected Health Information ("e-PHI," as defined below) on behalf of the Health Plan.

This Policy documents the Health Plan's efforts to comply with the HIPAA Security Rule, 45 CFR Part 164, Subpart C (the "Security Rule"). HIPAA and its implementing regulations require the Health Plan to:

- Ensure the confidentiality, integrity, and availability of the Health Plan's e-PHI that the Health Plan creates, receives, maintains or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of the e-PHI;
- Protect against any reasonably anticipated uses or disclosures of e-PHI that are not permitted by the HIPAA Privacy Rule; and
- Ensure workforce compliance with the Security Rule.

II. DEFINITIONS

A. Electronic Media means:

1 Electronic storage media on which data are or may be recorded electronically, including, for example, devices in computers (i.e., hard drives), and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

2 Transmission media used to exchange information already in electronic storage media. Transmission media include, among other things, the Internet, extranet, or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone, are not considered to be transmissions via electronic media, if the information being exchanged did not exist in electronic form immediately before the transmission.

B. Electronic Protected Health Information ("e-PHI") is Protected Health Information that is transmitted by, or maintained in, Electronic Media.

C. Exempt Information is e-PHI that is:

1. Summary Health Information, when used exclusively for (a) obtaining premium bids or (b) modifying, amending, or terminating the Health Plan;

2. Information on whether an individual is participating in the Health Plan, or is enrolled in or has disenrolled from an Insurer offered by the Health Plan; or

3. PHI disclosed to the Plan Sponsor under a signed authorization that meets the requirements of the HIPAA Privacy Rule.

D. Protected Health Information ("PHI") is the information that is subject to and defined in the Health Plan's HIPAA Policy (Policy No. 101).

E. Summary Health Information means information, that may be e-PHI, and:

1. that summarizes the claims history, claims expenses, or types of claims experienced by individuals for whom the Plan Sponsor has provided health benefits under the Health Plan; and

2. has been **de-identified** according to 45 C.F.R. § 164.514(b)(2)(i), *except that* geographic information described in 45 C.F.R. § 164.514(b)(2)(i)(B) needs only be aggregated to the level of a five-digit zip code.

III. APPOINTMENT OF SECURITY OFFICIAL

The Health Plan appoints the Benefits Division Director as the Plan's Security Officer. The Security Official is responsible for the development and implementation of the Health Plan's policies and procedures relating to security, including, but not limited to, this Policy.

IV. RISK ANALYSIS

The Health Plan has no employees. Except for functions performed by the Plan Sponsor using Exempt Information, all of the Health Plan's functions – including creating and maintaining its records and creating, receiving, maintaining, and transmitting e-PHI – are carried out by the Health Plan's Insurers.

The Health Plan does not create, receive, maintain, or transmit e-PHI; these functions are performed and controlled solely by the Insurers. The Health Plan does not own or control any of the equipment or media used to create, receive, maintain, and/or transmit e-PHI relating to Health Plan participants, beneficiaries, and covered dependents, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Insurers. The Health Plan does not control the Insurers' employees, agents, and subcontractors that have access to e-PHI relating to Health

Plan participants, beneficiaries, and covered dependents. The Health Plan has no ability to assess or modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI relating to Health Plan participants, beneficiaries, and covered dependents – that ability lies solely with the Insurers.

Given that (1) the Health Plan does not create, receive, maintain, or transmit e-PHI, (2) the Health Plan has no access to, or control over, the Insurers' employees, equipment, media, facilities, policies, procedures, or documentation affecting the security of e-PHI, and (3) all of the Insurers are themselves "Covered Entities" under the HIPAA Regulations with independent obligations to adopt and implement adequate security measures with respect to e-PHI, the Health Plan's policies and procedures – including this Policy – do not address the Security Rule standards and associated implementation specifications regarding:

- Security management process;
- Workforce security;
- Information access management;
- Security awareness and training;
- Security incident procedures;
- Contingency planning;
- Evaluation;
- Facility access controls;
- Workstation use;
- Workstation security;
- Device and media controls;
- Access controls;
- Audit controls;
- Integrity of e-PHI;
- Person or entity authentication; and
- Transmission security.

Further, because the Insurers do not disclose e-PHI to the Plan Sponsor other than Exempt Information, the Health Plan is not required to include provisions in the plan documents related to the Plan Sponsor’s safeguards for e-PHI it creates, receives, maintains, or transmits on the Health Plan’s behalf (45 C.F.R. § 164.314(b)(1)).

V. RISK MANAGEMENT

Based on the risk analysis described in Section 4, above, the Health Plan has made a reasoned and good-faith determination that it need not implement independent security measures reduce risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI related to Health Plan participants, beneficiaries, and covered dependents.

VI. BUSINESS ASSOCIATES

The Health Plan obtains signed Business Associate Agreements from all Business Associates in full compliance with the HIPAA Security Rule. Business Associates must agree to use appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of the Health Plan's e-PHI they create and/or receive on the Health Plan's behalf, and otherwise satisfy the requirements of the HIPAA Security Rule.. The Health Plan does not, and will not, allow a Business Associate to create or receive e-PHI on behalf of the Health Plan unless and until a compliant Business Associate Agreement has been executed.

If the Security Official knows of acts or patterns of activity by a Business Associate that are material violations of the Business Associate Agreement, the Security Official will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Security Official will determine, in consultation with the Health Plan's legal counsel, whether termination of the Business Associate Agreement is feasible. If not feasible, the Security Official will report the violation to the U.S. Department of Health and Human Services ("HHS").

VII. DOCUMENTATION

Except to the extent controlled by Insurers, the Health Plan's security policies and procedures, including this Policy, shall be documented, reviewed periodically, updated as necessary in response to environmental or operational changes affecting the security of e-PHI the Health Plan creates, receives, maintains, or transmits, and any changes required by the HIPAA regulations. All changes to these policies and procedures shall be documented promptly.

Policies, procedures, and other documentation controlled by the Health Plan may be maintained in either written or electronic form, and shall be maintained for at least six years from the date of creation or the date last in effect, whichever is later. If applicable state law requires a longer retention period, the Health Plan will comply.

The Health Plan shall make its policies, procedures, and other documentation relating to the Health Plan's e-PHI available to the Security Official, the Insurers, HHS, and the Plan

Sponsor, as well as other persons responsible for implementing the policies and procedures to which the documentation pertains.

VIII. SANCTIONS FOR VIOLATIONS OF SECURITY POLICIES

SDCERA employees who violate any of the Health Plan's security policies and procedures, including this Policy, will be subject to disciplinary action, up to and including termination of employment.

IX. 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.

X. EFFECTIVE DATE

This Policy is effective as of the date on which the HIPAA Security Rule 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	Revised
August 17, 2017	Revised