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 regulation, 45 CFR Part 164. HIPAA and its implementing regulations require the Health Plan to implement various security measures with respect to e-PHI. Specifically, the Health Plan will keep the Health Plan's e-PHI secure in accordance with the HIPAA security regulation. It is the Health Plan's policy, working together with its Insurers, to:

- Ensure the confidentiality, integrity, and availability of the Health Plan's e-PHI;
- 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 HIPAA;
- Ensure workforce compliance with the HIPAA security regulations and this Policy.

II. DEFINITIONS

A. Electronic Protected Health Information ("e-PHI") is protected health information that is transmitted by, or maintained in, electronic media.

B. Protected Health Information ("PHI") is the information that is subject to and defined in the Health Plan's HIPAA Policy (Policy No. 101). For purposes of this Policy, PHI does not include the following, referred to in this Policy as "Exempt Information:"

1. Summary health information, as defined by HIPAA's privacy rules, 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.

C. Electronic Media means:

1. Electronic storage media, including memory 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 (using Internet technology to link a business with information accessible only to collaborating parties), 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, because the information being exchanged did not exist in electronic form before the transmission.

III. APPOINTMENT OF SECURITY OFFICIAL

The Health Plan appoints the Director, Information Technologies, of SDCERA, 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 creation and maintenance of its records, are carried out by the Health Plan's Insurers.

The Health Plan does not own or control any of the equipment or media used to create, maintain, receive, and/or transmit e-PHI relating to the Health Plan, 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. Accordingly, the Insurers create and maintain all of the e-PHI relating to the Health Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive and/or transmit e-PHI relating to the Health Plan, and have control of their respective employees, agents, and subcontractors that have access to e-PHI relating to the Health Plan. 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 the Health Plan – that ability lies solely with the Insurers.

Given that the Health Plan has no access to, or control over, the Insurers' respective employees, equipment, media, facilities, policies, procedures, or documentation affecting the security of e-PHI relating to the Health Plan – and given that the Insurers are all, themselves, "Covered Entities" under the HIPAA privacy and security rules and are therefore themselves subject to an independent obligation to adopt and implement adequate security measures with respect to e-PHI (including e-PHI relating to the Health Plan) – the Health Plan's policies and procedures (including this Policy) do not address the following standards (including the implementation specifications associated with them) established under HIPAA and set out at Subpart C of 45 CFR Part 164:

- 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;
- Transmission security.

The Health Plan adopts the Insurers' own security policies and procedures as its own. And given that SDCERA has no access to e-PHI relating to the Health Plan, the Health Plan is not required to include provisions regarding the security of e-PHI in its plan document.

V. RISK MANAGEMENT

The Health Plan manages risks to its e-PHI by limiting vulnerabilities, based on its risk analysis, to a reasonable and appropriate level, taking into account the following:

- The size, complexity, and capabilities of the Health Plan;
- The Health Plan's technical infrastructure, hardware, software, and security capabilities;
- The cost of security measures; and
- The criticality of the e-PHI potentially affected.

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 take any additional security measures, other than the measures adopted by its Insurers to reduce risks to the confidentiality, integrity, and availability of the Health Plan's e-PHI.

VI. BUSINESS ASSOCIATES

To the extent that the Health Plan has Business Associates, it obtains signed Business Associate Agreements from all Business Associates in full compliance with the HIPAA security regulations. 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, and otherwise satisfy the requirements of the HIPAA security regulation. The Health Plan does not, and will not, disclose e-PHI to a Business Associate unless a 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 the Health Plan's e-PHI, 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.

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 HIPAA's security 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	Revised