



HIPAA PRIVACY POLICIES AND PROCEDURES
THE CALIFORNIA SCHOOLS
VOLUNTARY EMPLOYEES BENEFITS ASSOCIATION

The following policies and procedures are adopted by the California Schools Voluntary Employees Benefits Association (the VEBA) in accordance with the security and privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), were effective April 14, 2003, and revised effective June 10, 2009, and January 29, 2014.

These policies and procedures will be implemented with respect to the administration of the VEBA group health plans (VEBA Plan), offered to individuals (Plan Participants) through employers participating in the California Schools Voluntary Employees Benefits Association. The objectives of the policies and procedures outlined in this document are to define how the VEBA Plan may handle and share Protected Health Information (PHI).

HIPAA Background: The federal government has defined and standardized practices and procedures that describe how medical information may be used and disclosed and how individuals can access their personal information and ensure their rights are protected. This federal law:

- Defines the groups that review and handle health information;
- Protects individually identifiable health information;
- Provides individuals with right to access their own health information;
- Requires authorization to use and disclose health information; and
- Ensures Plan Participants receive adequate notice of their privacy rights.

The VEBA Plan: These policies and procedures will apply to the group health plans sponsored and maintained by the VEBA Plan.

These policies and procedures are comprised of two parts. Part I sets forth the **General Rules** applicable to the VEBA Plan. Part II sets forth the **Policies and Procedures** applicable to the VEBA Plan.

PART I -- GENERAL RULES

The California Schools Voluntary Employees Benefits Association has established and maintains a methodology for consistent development, training, review, approval, assessment and updates of policies and procedures as they pertain to HIPAA Privacy regulations applicable to the VEBA Plan.

The California Schools Voluntary Employees Benefits Association (the VEBA) hereby designates the California VEBA Administrator (VEBA Administrator) as the entity responsible to oversee and monitor the overall implementation of HIPAA policies and procedures applicable to the VEBA Plan. The VEBA Administrator may delegate actual performance of the duties to a Privacy Officer. For purposes of these policies and procedures, The VEBA Administrator includes the Privacy Officer, and other key personnel specifically identified as having access to PHI.

Protected Health Information: For purposes of these policies and procedures, protected health information (“PHI”) means information that (1) is created or received by the VEBA Plan and relates to the past, present, or future physical or mental health condition of a Plan Participant; the provision of health care to a Plan Participant; and (2) identifies the Plan Participant or provides a reasonable basis for identifying such Plan Participant. PHI includes information of persons living or deceased. PHI will not be used in conjunction with any employment-related decisions, such as hiring, promotion, termination, leave of absence, or compliance with the Americans with Disabilities Act without proper authorization from the employee, or any other records excluded under the Department of Health and Human Services (“DHHS”) privacy regulations.

In order to provide for or permit the disclosure of PHI by the VEBA Plan, the VEBA Plan will ensure that uses and disclosures of PHI are consistent with HIPAA Privacy regulations as follows:

- Describe the permitted uses and disclosures of PHI by the VEBA Plan;
- Specify that disclosure is permitted only in accordance with HIPAA requirements;
- Provide adequate firewalls which identify the employees, classes of employees or other person(s) under the VEBA Plan’s control who will have access to PHI; and
- Provide an effective mechanism for resolving any issues of non-compliance by the employees or class of employees who will have access to PHI.

Training: The Privacy officer will be responsible for training personnel of the VEBA Administrator who have access to PHI with respect to these policies and procedures and the privacy requirements of HIPAA generally. Additional training will also be provided to the extent necessary and appropriate to permit such personnel to carry out the specific administrative functions assigned to each of them. Each new person will be trained within a reasonable period of time following his/her commencement as an individual having access to PHI. Ongoing training for all personnel will be conducted as necessary.

Non-Compliance/Discipline: If at any time the Privacy Officer determines that any person is not in compliance with these policies and procedures, the Privacy Officer may conduct additional training. The Privacy Officer will also maintain a separate record of such noncompliance and periodically monitor any corrective procedures taken to ensure compliance. To the extent necessary, the Privacy Officer will discipline or remove the individual.

Non-Retaliation: The VEBA Plan will not take any retaliatory or intimidating action against a VEBA Plan Participant for exercising his/her rights under HIPAA or these policies and procedures. Further, a Plan Participant's treatment under the VEBA Plan may not be conditioned upon a Plan Participant's failure to waive his/her privacy rights.

Amendment to Policies and Procedures: The VEBA Plan, reserves the right to amend or modify these procedures from time to time, either prospectively or retroactively and without notice to Plan Participants.

No Third Party Rights: No third party rights (including but not limited to rights of VEBA Plan Participants or VEBA Plan Business Associates are intended to be created by these policies and procedures.

PART II – POLICIES AND PROCEDUES

Permitted Access and Disclosure of PHI: The VEBA Plan will have access to and may use and disclose PHI only for the purpose of the following:

- **Payment:** The VEBA Plan will use or disclose PHI to fulfill its responsibilities for coverage and providing benefits as established under the VEBA Plan. For example, the VEBA Plan may disclose PHI when a provider requests information regarding eligibility for benefits under the VEBA Plan, or it may use PHI information to determine if a treatment that is received was medically necessary.
- **Health Care Operations:** The VEBA Plan will use or disclose PHI to support the VEBA Plan's business functions. For example, the VEBA Plan may use or disclose PHI (1) to evaluate the VEBA Plan performance; (2) evaluate VEBA Plan benefit provider performance; (3) in underwriting, premium rating, and other activities relating to creation, renewal, or replacement of a contract of health insurance or benefits; (4) for business planning; and (5) for business management and general administrative activities of the VEBA Plan.
- **Other Covered Entities:** The VEBA Plan may use or disclose PHI to assist health care providers in connection with their treatment or payment activities, or to assist other covered entities in connection with certain health care operations. For example, the VEBA Plan may disclose PHI to a health care provider when needed by the provider to render treatment to the Plan Participant, and the VEBA Plan may disclose PHI to another covered entity to conduct health care operations in the areas of quality assurance and improvement activities, or accreditation, certification, licensing, or credentialing. This also means that the VEBA Plan may disclose or share PHI with other health care programs or insurance carriers (such as Medicare, PacifiCare of California, Kaiser, etc.) in order to coordinate benefits, if the Plan Participant has other health insurance or coverage.

- *Required by Law:* The VEBA Plan may use or disclose PHI to the extent required by federal, state, or local law.
- *Public Health Activities:* The VEBA Plan may use or disclose PHI for public health activities that are permitted or required by law. For example, it may use or disclose information for the purpose of preventing or controlling disease, injury, or disability, or it may disclose such information to a public health authority authorized to receive reports of child abuse or neglect. The VEBA Plan also may disclose PHI, if directed by a public health authority, to a foreign government agency that is collaborating with the public health authority.
- *Health Oversight Activities:* The VEBA Plan may disclose PHI to a health oversight agency for activities authorized by law. For example, these oversight activities may include audits; investigations; inspections; licensure or disciplinary actions; or civil, administrative, or criminal proceedings or actions. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and government agencies that ensure compliance with civil rights laws.
- *Lawsuits and Other Legal Proceedings:* The VEBA Plan may disclose PHI in the course of any judicial or administrative proceeding or in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized). If certain conditions are met, the VEBA Plan may also disclose PHI in response to a subpoena, a discovery request, or other lawful process.
- *Abuse or Neglect:* The VEBA Plan may disclose PHI to a government authority that is authorized by law to receive reports of abuse, neglect, or domestic violence. Additionally, as required by law, if the VEBA Plan believes a Plan Participant has been a victim of abuse, neglect, or domestic violence, it may disclose PHI to a governmental entity authorized to receive such information.
- *Law Enforcement:* Under certain conditions, the VEBA Plan may disclose PHI to law enforcement officials for law enforcement purposes. These law enforcement purposes include, by way of example (1) responding to a court order or similar process; (2) as necessary to locate or identify a suspect, fugitive, material witness or missing person; or (3) as relating to the victim of a crime.
- *Coroners, Medical Examiners, and Funeral Directors:* The VEBA Plan may disclose PHI to a coroner or medical examiner when necessary for identifying a deceased person or determining a cause of death. The VEBA Plan also may disclose PHI to funeral directors as necessary to carry out their duties.
- *Organ and Tissue Donation:* The VEBA Plan may disclose PHI to organizations that handle organ, eye, or tissue donation and transplantation.
- *Research:* The VEBA Plan may disclose PHI to researchers when (1) their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of PHI; or (2) the research involves a limited data set which includes no unique identifiers (information such as name, address, social security number, etc., that can identify the Plan Participant).

- *To Prevent a Serious Threat to Health or Safety:* Consistent with applicable laws, the VEBA Plan may disclose PHI if disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. It may disclose PHI if it is necessary for law enforcement authorities to identify or apprehend an individual.
- *Military:* Under certain conditions, the VEBA Plan may disclose PHI to authorized federal officials for conducting national security and intelligence activities, and for the protection of the President, other authorized persons, or heads of state.
- *Inmates:* If the VEBA Plan Participant is an inmate of a correctional institution or under the custody of a law enforcement official, the VEBA Plan may disclose PHI to the correctional institution or to a law enforcement official for (1) the institution to provide health care to the Plan Participant; (2) the Plan Participant's health and safety, and the health and safety of others; or (3) the safety and security of the correctional institution.
- *Workers' Compensation:* The VEBA Plan may disclose PHI to comply with workers' compensation laws and other similar programs that provide benefits for work-related injuries or illnesses.
- *Others Involved In a VEBA Plan Participant's Health Care:* The VEBA Plan may disclose PHI to a friend or family member that is involved in the health care of a VEBA Plan Participant unless the Plan Participant objects or requests a restriction (in accordance with the process described below under "Right to Request Restrictions"). The VEBA Plan also may disclose PHI to an entity assisting in a disaster relief effort so that the family of a Plan Participant can be notified about the Plan Participant's condition, status, and location. If the Plan Participant is not present or able to agree, the VEBA Plan may determine whether the disclosure is in the Plan Participant's best interest.
- *Disclosures to the VEBA Plan Participant:* The VEBA Plan is required to disclose to the Plan Participant or their personal representative most of the Plan Participant's PHI when it is requested. The VEBA Plan will disclose PHI to an individual who has been designated by the Plan Participant as his/her personal representative and who has qualified for such designation in accordance with relevant law. Prior to such a disclosure, however, the VEBA Plan must be given written documentation that supports and establishes the basis for the personal representation. The VEBA Plan may elect **not** to treat the person as the Plan Participant's personal representative if (1) there is reasonable belief that the Plan Participant has been, or may be, subjected to domestic violence, abuse, or neglect by such person; (2) treating such person as the Plan Participant's personal representative could endanger the Plan Participant; or (3) the VEBA Plan determines, in the exercise of its professional judgment, that it is not in the Plan Participant's best interest to treat the person as the personal representative.

"Minimum Necessary" Disclosure: When using or disclosing PHI or when requesting PHI from another covered entity, the VEBA Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the permitted use, disclosure, or request, taking into consideration practical and technological limitations. In particular, the VEBA Plan will make a determination as to whether disclosure of the Plan Participant's name and/or social security number is necessary and will blackout or delete all unnecessary information. The "minimum necessary" standard does not apply to any of the following;

- Uses or disclosures made to the covered Plan Participants;
- Uses or disclosures made pursuant to an authorization of the covered Plan Participant;
- Disclosures made directly to the Department of Labor;
- Uses or disclosures required by law; or
- Uses or disclosures required to comply with HIPAA.

All other disclosures will be reviewed on an individual basis to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Safeguarding PHI: The VEBA Plan will use all reasonable efforts to secure PHI, including locking file drawers, clearing work areas of PHI, not disclosing passwords, and ensuring that computer screens log-out after non-use. Personnel having access to PHI may not access PHI from home or offsite computers without the permission of the Privacy Officer, who will grant permission only if the home or offsite computer meets the required security standards.

All written PHI records received by the VEBA Plan will be maintained in a secure location at the VEBA Administrator's office and only personnel of the VEBA Administrator, to the minimum extent necessary to accomplish a permitted use or purpose, will have access to such information. PHI that is not in an electronic format shall either be maintained in a locked file drawer or other secure location. PHI maintained in an electronic format will be password-protected and only those personnel of the VEBA Administrator who have a need to know will have access to the information.

The VEBA Plan will destroy all PHI received from a group health plan or other person or entity, and retain no copies of such PHI when no longer needed for the purpose for which disclosure was made. If destruction is not feasible, the VEBA Plan will limit further uses and disclosures to those purposes that make the destruction infeasible.

The Privacy Officer will be responsible for informing personnel within the VEBA Administrator's information technology department of their responsibilities and obligations with respect to HIPAA Privacy requirements. Such personnel will be notified that they are subject to discipline, including termination, if they improperly access PHI.

Mitigation of Improper Disclosures: The VEBA Plan will mitigate, to the extent practicable, any harmful effect that is known by the VEBA Plan to have occurred as a result of a use or disclosure of PHI in violation of HIPAA Privacy requirements by either the VEBA Plan or its Business Associates.

Individual Right to Receive Notice of Breach of Unsecured PHI: If the security of a Plan Participant's unprotected PHI is breached, the VEBA Plan will notify the affected Participant of it no later than the time prescribed by applicable law or regulation

Authorizations: Except as permitted under DHHS Reg. § 164.506 (relating to uses and disclosure of PHI to carry out treatment, payment or health care operations), or DHHS Reg. § 164.512 (relating to uses and disclosures for public policy reasons), disclosures of PHI may only be made upon the written authorization of the covered Plan Participant. Each such authorization must be in writing on a form prescribed by the Privacy Officer. Such authorizations shall be compiled and delivered to the Privacy Officer or his/her designee on a quarterly or more frequent basis. Such authorizations shall be maintained for a minimum period of six years following the date of disclosure.

A VEBA Plan Participant may revoke a prior authorization in writing at any time, except to the extent that the VEBA Plan has taken action in reliance on the original authorization; or if the original authorization was obtained as a condition of obtaining insurance coverage, applicable law provides the insurer with the right to contest a claim under the policy.

The VEBA Plan will not condition the provision of benefits or eligibility under the Plan upon receipt of an authorization from a Plan Participant, unless the authorization is sought for determining the Plan Participant's eligibility or enrollment under the VEBA Plan or determining the VEBA Plan's underwriting or risk rating.

Disclosure to Personal Representatives: The VEBA Plan may disclose PHI to a personal representative of the Plan Participant if the VEBA Plan receives:

- Authorization from the Plan Participant to disclose PHI to the personal representative;
- A written power of attorney for health care purposes, notarized by a notary public;
- A court order of appointment of the person as the conservator or guardian of the individual; or
- The personal representative is a parent of a minor child

The VEBA Plan reserves the right to deny access to a Plan Participant's PHI to a personal representative if in the VEBA Plan's judgment it would not be in the best interest of the Plan Participant in light of the surrounding circumstances.

Individual Right to Restrict Disclosure: Each Plan Participant will have the right to request in writing that the VEBA Plan not use or disclose his/her PHI for any otherwise permitted purpose. It shall be the policy of the VEBA Plan that such individual requests will normally be denied unless the Privacy Officer or his/her designee determines that special circumstances warrant an exception. If the individual's request to restrict the disclosure of PHI is granted, then the VEBA Plan will not use or disclose such information in violation of the requested restriction except as follow: (1) to carry out medical emergency treatment on behalf of the Plan Participant; (2) to facilitate the treatment, payment or health care operations of the Plan; or (3) for any other permitted purpose under DHHS Reg. § 164.510(a) (relating to uses and disclosures for the directory of a health care provider's facility) or DHHS Reg. § 164.512 (relating to uses and disclosures for public policy reasons).

Individual Right to Request Alternative Means or Location of Communication: The VEBA Plan will honor a Plan Participant's reasonable request to receive confidential communications of his or her PHI by alternative means or at an alternative location, if the Plan Participant states that the disclosure of all or part of that information could endanger the Plan Participant. Such request must be made in writing and directed to the Privacy Officer. As appropriate, the Privacy Officer will cause reasonable steps to be taken to honor the Plan Participant's request. If a Plan Participant requests that his/her PHI be communicated by alternative means or at an alternative location for a reason other than the endangerment of the Plan Participant, the Privacy Officer will not normally grant such request unless the circumstances warrant a special exception to the VEBA Plan's normal administrative process.

Individual Right to Access PHI: Each Plan Participant shall have a right to inspect and obtain a copy of his/her PHI so long as such information is maintained in a designated record set (as

defined below). The requested information will be provided within 30 days of the request or within 60 days if the information is maintained off-site. Each Plan Participant (or his/her personal representative) will be required to complete a form prescribed by the Privacy Officer to request access to PHI. All such requests must be directed in writing to the Privacy Officer. If access is denied, the Plan Participant or his/her representative will be provided with a written denial setting forth the basis for the denial and any steps that he/she may take to request a review.

Under federal law, a Plan Participant may not inspect or copy the following records: (1) psychotherapy notes; (2) information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and (3) PHI that would not otherwise be available for inspection under the DHHS regulations. Depending on the circumstances, a decision to deny access may be reviewable. In some, but not all circumstances, the Plan Participant may have a right to have this decision reviewed.

A “designated record set” means and includes (1) the medical records and billing records about an individual maintained by or for a covered health care provider; (2) enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for a group health Plan; or (3) other information used in whole or in part by or for the group health plan to make decisions about an individual.

Individual Right to Amend PHI: Each Plan Participant shall have the right to request an amendment of his/her PHI for so long as it is maintained in a designated record set. All requests to amend PHI should be directed to the Privacy Officer in writing. The Plan Participant’s request to amend his/her PHI may be denied, if the Privacy Officer determines that the PHI that is the subject of the request (1) was not created by the VEBA Plan (unless the Plan Participant provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the requested amendment); (2) is not part of the designated record set; (3) would not otherwise be available for inspection under the DHHS regulations; or (4) is accurate and complete.

Accounting for Disclosures: The Privacy Officer or his/her designee will be responsible for compiling and maintaining a master list of disclosures other than those listed below. Upon request to the Privacy Officer and in accordance with DHHS Reg. § 164.528, a Plan Participant may request an accounting of all disclosures of PHI during the six-year period prior to the date on which the accounting is requested, except for the following:

- Disclosures that are for purposes of carrying out treatment, payment and health care operations;
- Disclosures that are to the covered Plan Participant about themselves;
- Disclosures pursuant to a valid authorization of the Plan Participant;
- Disclosures that occurred prior to the HIPAA compliance date for the VEBA Plan;
- Disclosures incident to any other use or disclosure permitted or required by the DHHS regulation (for example, disclosures mandated for national security or national

intelligence, disclosures to correctional institutions or law enforcement professionals, disclosures to the Department of Health and Human Services to determine compliance, etc.).

During a twelve-month period, one accounting is available free of charge. There will be a charge to cover the VEBA Plan's costs for additional requests within that twelve-month period.

Distribution of Privacy Notice: Existing Plan Participants will be provided with a notice (paper or electronic) of their privacy rights and the uses and disclosures of PHI that may be made by the VEBA Plan and the Plan's legal duties with respect to PHI no later than the time prescribed by applicable law. The Privacy Officer will be responsible for amending the privacy notice from time to time as the Privacy Officer deems necessary to reflect amendments to these policies and procedures.

Disclosures of De-Identified Information, Summary Information, and Limited Data Sets: The VEBA Plan may disclose de-identified information, which is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. The VEBA Plan may disclose summary information for purposes of determining plan design and obtaining bids from providers. The Privacy Officer will be responsible for determining that the information disclosed constitutes either de-identified information or summary information. In accordance with DHHS regulations, the VEBA Plan may also use or disclose a "limited data set" to another covered entity for purposes of research, public policy or health care operations, if the VEBA Plan obtains satisfactory assurance, in the form of a data use agreement, that the limited data set recipient will only use or disclose for such permitted purpose.

Relationships with Third Party Vendors: All third party vendors (Business Associates) providing services involving PHI to, related to, or on behalf of the VEBA Plan will be required to enter into Business Associate contracts no later than the effective date of HIPAA's privacy regulations (or, if later, the date they first commence services on behalf of the Plan). PHI will not be disclosed to any such vendor in the absence of a Business Associate contract. The contract shall include provisions necessary to require the Business Associates to comply with HIPAA privacy rules. If the VEBA Plan becomes aware of a Business Associate's pattern of activity or practice that constitutes a material breach or violation of its obligation under the Business Associate agreement, the VEBA Plan will take steps to cure the breach or end the violation. If these steps are unsuccessful, the VEBA Plan will either (1) terminate the contract or arrangement, if feasible; or (2) if not feasible to terminate, report the problem to the Secretary of the Department of Health and Human Services.

Business Associates include, but are not limited to, a person/entity who performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information or any other regulated function or activity, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business Associates may also provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates.

Periodic Monitoring/Audits: The Privacy Officer will perform an overall assessment of compliance with these policies and procedures no less frequently than annually. The Privacy Officer may also require an internal or external audit of the policies and procedures to ensure compliance with HIPAA privacy rules.

Handling of Complaints: All complaints regarding PHI disclosures must be reported to the Privacy Officer. The Privacy Officer will be responsible for resolving any disputes and taking corrective action. The Privacy Officer will maintain a log of all such complaints and a summary of the resolution for the matter. Such log will be maintained for a minimum period of six years.

A Plan Participant who believes a covered entity is not complying with HIPAA privacy rules has a right to file a complaint with the Secretary of the U. S. Department of Health and Human Services at its Region IX office, located at 90 7th Street, Suite 4-100, San Francisco, California 94103.