

This Business Associate Privacy Agreement (this “**Agreement**”), effective _____, is entered into by and between CHOICE Administrators®, Inc. (and its Affiliates, as defined herein) (collectively, the “**Company**”) and the entity identified on the signatory page (“**Broker**”), (collectively, the “**Parties**”). This Agreement is drafted for the express purpose of complying with the privacy requirements of the California Insurance Information and Privacy Protection Act (CIC 791 *et seq.*, “**IIPPA**”), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 1501 *et seq.*, the “**GLBA**”) and regulations adopted by the California Department of Insurance to implement IIPPA and the GLBA (10 C.C.R. §§ 2689.1 *et seq.*, the “**IIPPA Privacy Regulations**”), the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”) and regulations adopted by the U.S. Department of Health and Human Services to implement HIPAA (45 CFR Parts 160-64, the “**HIPAA Privacy Regulations**”) to ensure the integrity and confidentiality of individually identifiable personal and health information that Broker may collect, create for or receive from the Company (collectively, the “**Privacy Rule**”). Additional terms and conditions in accordance with local privacy ordinances shall be set forth in an Addendum. The term “**Privacy Rule**” also includes local privacy ordinances.

Whereas, Company is a Business Associate to various health plans that are Covered Entities; and

Whereas, As a Business Associate, Company is obligated to safeguard the privacy and security of Protected Health Information received by or created for or on behalf of such Covered Entities; and

Whereas, Company has engaged Broker to perform certain functions for and on behalf of Company and/or such a Covered Entity pursuant to which Broker shall receive certain Protected Health Information of such a Covered Entity; and

Whereas, Company desires to secure Broker’s assurances that it will safeguard the privacy and security of such Protected Health Information and take other actions in order to assist Company in meeting its obligations to such Covered Entities and as a Business Associate under HIPAA.

A. Definitions

- 1 “**Affiliate**” or “**Affiliated**” means a person that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person.
- 2 “**Breach**” (with respect to Unsecured Health Information) shall have the meaning set forth in 45 C.F.R. § 164.402, as amended from time to time, and currently means the acquisition, access, use or disclosure of protected health information in a manner not permitted under the Privacy or Security Standards and which compromises the security or privacy of the Health Information.
- 3 “**Business Associate**” means an individual or entity that performs a function or activity on behalf of, or provides a service to a Covered Entity (as defined herein), that involves the collection, creation, use or disclosure of Personal and Health Information.
- 4 “**Covered Entity**” means a health plan, health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA Privacy Regulations.
- 5 “**De-Identify**” or “**De-Identification**” means Health Information that does not identify an individual and with respect to which there is no reasonable basis to believe that such information can be used to identify an individual.
- 6 “**Designated Record Set**” means a group of records maintained by or for a Covered Entity comprising the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Covered Entity or Business Associate of the Covered Entity or used, in whole or in part, by or for the Covered Entity to make decisions about individuals. For purposes of this Section, the term “record” includes any item, collection, or grouping of information that contains Personal and Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity or the Company.
- 7 “**Electronic Health Information**” means Health Information that is transmitted or maintained in electronic media.
- 8 “**Electronic Media**” means:
 - (i) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
 - (ii) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), 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 of paper, via facsimile, and of 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.
- 9 “**Health Information**” means “Protected Health Information” as this term is defined under the HIPAA Privacy Regulations, and includes any information in possession of or derived from a physician or other provider of health care or a health care service plan regarding an individual’s medical history, mental or physical condition or treatment, as well as information related to the past, present or future payment for the provision of healthcare.
- 10 “**Limited Data Set**” means Health Information that excludes the following direct identifiers of the individuals or of relatives, employers or household members of the individual: (i) names; (ii) postal address information, other than town or city, State and Zip Code; (iii) telephone numbers; (iv) fax numbers; (v) electronic mail addresses; (vi) social security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images.
- 11 “**Personal and Health Information**” means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual’s character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristics. Individually identifiable information includes the individual’s name, address, electronic mail address, telephone number, social security number and other information, alone or in combination with other publicly available information, which reveals the individual’s identity. Personal information includes the individual’s nonpublic personal financial information.
- 12 “**Security Standards**” shall mean the Security Standards for the Protection of Electronic Health Information, 45 CFR Part 160 and Part 164, Subparts A and C.
- 13 “**Unsecured Health Information**” shall mean unsecured PHI as set forth in 45 CFR § 164.402, as amended from time to time, and currently means Health Information that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services.

B. Privacy of Personal and Health Information

1. **Permitted Uses and Disclosures.** Broker is permitted or required to use or disclose Health Information or Personal and Health Information it collects, creates for or receives from the Company only as follows:
 - a) **Functions and Activities on the Company’s Behalf.** Broker is permitted to use and disclose the minimum necessary Health Information or Personal and Health Information it collects, creates for or receives from the Company in order to provide services to the Company, any Covered Entity for which the Company and/or Broker are Business Associates, or another Business Associate of such a Covered Entity.
 - b) **Broker’s Operations.** Broker may use and disclose the minimum necessary Health Information or Personal and Health Information it collects, creates for or receives from the Company as necessary in order to perform Broker’s proper management and administration, or to carry out Broker’s legal responsibilities. If Broker discloses such Health Information or Personal and Health Information to an agent, a subcontractor or other third party, then Broker shall obtain reasonable assurances from the agent, subcontractor or other third party to which Broker discloses such Health Information or Personal and Health Information that agent, subcontractor or other third party shall: (i) hold such Health Information or Personal and Health Information in confidence and use or further disclose it only for the purposes for which Broker disclosed it to the agent, subcontractor or other third party or as required by law; and (ii) notify Broker (who shall in turn promptly notify the Company) of any instances of which the agent, subcontractor or other third party becomes aware that the confidentiality of such Health Information or Personal and Health Information was breached.

2. **Prohibition on Unauthorized Use or Disclosure.** Broker shall neither use nor disclose Health Information or Personal and Health Information it collects, creates for or receives from the Company, except as permitted or required by this Agreement, or as permitted or required by law.
3. **Compliance with the Company's Confidentiality/Privacy Policies.** Broker shall comply with the Company's Privacy Statement included at the end of this document and other Confidentiality, Privacy, and Security Policies the company may make available to the broker over the term of this agreement to meet applicable legal requirements.
4. **De-Identification of Information/Creation of Limited Data Set.** Broker shall not De-Identify Health Information it creates or receives for or from the Company, and shall not use or disclose such de-identified information, unless such de-identification is expressly permitted under the terms and conditions of this Agreement for services to be provided by Broker to the Company related to the Company's activities for purposes of "treatment," "payment" or "health care operations," as those terms are defined under the HIPAA Privacy Regulations. Broker further agrees that it will not create a Limited Data Set using Health Information it creates or receives for or from the Company, nor use or disclose such Limited Data Set unless: (i) such creation, use or disclosure is expressly permitted under the terms and conditions of this Agreement; and (ii) such creation, use or disclosure is for services provided by Broker that relate to the Company's activities for purposes of "payment" or "health care operations", as those terms are defined under the HIPAA Privacy Regulations.
5. **Information Safeguards.** Broker shall develop, implement, maintain and use appropriate administrative, technical and physical safeguards, in compliance with applicable state and federal laws, to preserve the confidentiality of and to prevent unauthorized disclosures of Health Information or Personal and Health Information collected, created or received for or from the Company. Broker shall document and keep such safeguards current and, upon the Company's reasonable request, shall provide the Company with a copy of policies and procedures related to such safeguards.

C. Personal and Health Information Access, Amendment and Disclosures

1. **Access.** Broker shall, upon the Company's reasonable request permit, within ten (10) business days of receipt of request, an individual (or the individual's personal representative) to inspect and obtain copies of any Health Information or Personal and Health Information about the individual which Broker collected, created or received for or from the Company and that is in Broker's custody or control.
2. **Amendment.** Broker shall, upon receipt of notice from the Company, promptly amend or permit the Company access to amend any portion of an individual's Health Information or Personal and Health Information which Broker collected, created or received for or from the Company and that is in Broker's custody or control.
3. **Disclosures.** Broker shall document each disclosure it makes of an individual's Health Information or Personal and Health Information to a third party. Moreover, for purposes of this Section, "disclosure" includes: 1) any legal disclosure; 2) any illegal, inadvertent, wrongful, or negligent disclosure; and 3) any instance in which access was provided to an unauthorized third party to an individual's Health Information or Personal and Health Information. For the purposes of this Agreement, "legal disclosure" includes, but is not limited, any disclosures to law enforcement or other governmental authority pursuant to law and in response to a facially valid administrative or judicial order, such as a search warrant or subpoena.
4. **Disclosure Reporting.**
 - a) **Legal.** In a timely manner but not later than 30 days from the date of the disclosure, Brokers shall forward to the Company a report of such disclosures, as required by 45 CFR §164.528; however, this requirement shall not apply if Broker has not made any such disclosures. Such report shall include the applicable individual's name, the person to whom the Health Information or Personal and Health Information was disclosed, what was disclosed, why the information was disclosed, and the date of such disclosure.
 - b) **Illegal, Inadvertent or Wrongful Disclosure.** Broker shall report to the Company any use or disclosure of Health Information or Personal and Health Information not permitted by this Agreement or that would be in violation of the Privacy Rule if made by Company. Business Associate shall make the report to the Company not more than twenty-four (24) hours after Broker learns of such non-permitted use or disclosure. Broker shall report such disclosure in accordance with Section D of this Agreement.
 - c) **Termination of Agreement.** Upon termination of this Agreement, Broker shall provide to the Company one final report of any and all disclosures made of all individuals' Health Information or Personal and Health Information.
5. **Inspection of Books and Records.** Broker shall make its internal practices, books and records, relating to its use and disclosure of the Personal and Health Information it collects, creates or receives for or from the Company, available to the U.S. Department of Health and Human Services or to the California Insurance Commission to determine the Company's compliance, as a Business Associate, with the provisions of the HIPAA Privacy Regulations or the HIPAA Privacy Regulations, whichever is applicable.
6. **Designated Record Set.** Broker agrees that all Health Information or Personal and Health Information received by or created for the Company shall be included in an individual's Designated Record Set. Broker shall maintain such Designated Record Set with respect to services provided to an individual under this Agreement, and shall allow such individual to access the Designated Record Set as provided in the HIPAA Privacy Regulations.

CI. Breach

1. **Generally** In furtherance of Broker's obligation under Sections C.3. and C.4 above, Broker Business Associate shall, within five (5) days of becoming aware of a Breach of Unsecured PHI or any other disclosure of protected health information in violation of this Agreement by Broker Business Associate, its officers, directors, employees, contractors or agents or by a third party to which Broker Business Associate disclosed protected health information pursuant to Broker Business Associate Agreement, report any such Breach or disclosure to the Company. Such notification shall include, to the extent possible, the identification of each individual whose protected health information has been, or is reasonably believed by Broker Business Associate to have been, accessed, acquired, used, or disclosed during the Breach. In addition, Broker Business Associate shall provide Company with the following information, to the extent available at the time initial notice to Company is provided, or promptly thereafter as such information becomes available:
 - A brief description of what happened, including the date of the Breach or wrongful disclosure and the date of discovery
 - A description of the type of protected health information that was involved (e.g., name, Social Security Number, procedure, diagnosis, treatment, etc.)
 - The steps that BROKER BUSINESS ASSOCIATE recommends that the individual should take to protect himself or herself
 - A brief description of the steps that BROKER BUSINESS ASSOCIATE is taking to investigate, mitigate harm, and protect against future similar breaches
 - Any such other information, including a written report, as the Company may reasonably request
2. **Termination of Agreement.** This Agreement shall terminate automatically in the event that Broker ceases performing services for or on behalf of Company or in the event that Broker otherwise ceases to be a Business Associate of either the Company or a Covered Entity with respect to whom the Company is a Business Associate. The Company may also, in addition to other available remedies, terminate this Agreement if Business Associate has materially breached any provision(s) of this Agreement and has failed to cure or take any actions to cure such material breach within five (5) calendar days of the Company informing Broker of such material breach. The Company shall exercise this right to terminate by providing Broker written notice of termination, which termination shall include the reason for the termination. Any such termination shall be effective immediately (following any applicable cure period) or at such other date specified in the Company's notice of termination.
 - a) **Obligations upon Termination.** Upon termination, cancellation, expiration or other conclusion of this Agreement or any other agreements for any reason, Broker shall comply with applicable Privacy Rule requirements regarding the return or destruction of Health Information or Personal and Health Information.
 - b) **Continuing Privacy Obligation.** Broker's obligation to protect the privacy of the Health Information or Personal and Health Information shall be continuous and survive termination, cancellation, expiration or other conclusion of this Agreement.



PRIVACY STATEMENT

CHOICE Administrators® is proud to provide quality employee benefit products and services to our customers. Keeping your personal information secure and protecting your privacy rights are important to you, and it is one of our top priorities.

This statement tells you about the information we request from our customers. It also tells you how we safeguard the personal information and protect the privacy rights of our current and former customers.

Our Privacy Commitment to You

CHOICE Administrators will safeguard your personal information and protect the privacy rights of our customers in accordance with state and federal laws. We will accomplish this in ways that are reasonable and consistent with sound business practices.

Protecting Your Health Information

We do not share your personal health information (such as medical questionnaires) except when necessary to conduct underwriting reviews at the time of your Employer's initial enrollment through CHOICE Administrators or upon an Employer requested underwriting review at a subsequent renewal. In certain circumstances, we may share your personal health information if permitted or required by law.

CHOICE Administrators is committed to protecting the confidentiality and security of your private health information. We maintain physical, electronic, and process safeguards that restrict unauthorized access to your personal health information. These security procedures include locked files and information system security measures such as user passwords, data encryption or firewall technology.

CHOICE Administrators employees are required to comply with our policies and procedures to protect the confidentiality of your personal health information. Any employee who violates our privacy policy is subject to a disciplinary process. Employee access to private information is limited on a business "need-to-know" basis such as: when necessary to conduct underwriting reviews, or for anonymous statistical analysis.

Information About Our Customers

CHOICE Administrators receives information about you in order to provide customer service, offer new products or services, administer our products, and fulfill other legal and regulatory requirements. We will provide you with access to this information and the ability to review, amend, correct or copy this information, if we are required to do so under state and federal law. The methods we use to protect this information are similar to those described above to protect your health information.

The information we receive may vary by product; therefore, the examples that follow may not apply to all customers but are designed to show the general categories of information that may be received and maintained by CHOICE Administrators:

- Information provided by you on applications, forms, surveys and our Web sites, such as your name, address, date of birth, Social Security number, gender, marital status and dependents.
- Information provided by your employer.
- Information about your transactions and experiences with CHOICE Administrators such as: products or services purchased, account balances, payment history, policy coverage, and premiums.

Information Shared Within the Word & Brown Family of Companies

While understanding the importance of protecting your personal information, certain information will need to be shared during the normal course of business. We may disclose to the extent permitted by law the personal information we receive about you, as described above, within the Word & Brown Family of Companies.

Information Shared With Others

We may disclose the personal information we receive, as described above, to the following types of third parties:

- Other third parties as permitted or required by law, such as for compliance with a subpoena, fraud prevention, or inquiries from state or federal regulatory agencies.
- Financial service companies with whom we have agreements, such as: insurance companies, insurance brokers or agents, administrators, and service providers.

We maintain written contracts with third parties to help ensure that the personal information we share about our customers is used for a legitimate business purpose.

Access and Amendment of Your Records

You have the right to access and amend your records. You may exercise this right by requesting to us in writing to access and/or amend your records. Please send such requests to:

CHOICE Administrators
Attn: Legal Department
721 South Parker, Suite
200 Orange, CA 92868

Changes to Our Notice of Privacy Policy and Insurance Information Practices

We reserve the right to change our privacy policies and insurance information practices. If we make any changes to our policies or practices, we will provide you with a copy of a revised notice as required by applicable law.

Our Commitment

CHOICE Administrators values you as a customer, and we are committed to bringing you products and services that help you to feel healthier and more secure. Our goal is to always use your information in a responsible business manner. If there are state and federal law requirements that prohibit sharing your information without your written permission, CHOICE Administrators will comply with those requirements.