



LONE STAR
ALLIANCE_{RRG}

BUSINESS ASSOCIATE AGREEMENT

BETWEEN LONE STAR ALLIANCE RRG AND POLICYHOLDERS

Recitals

Lone Star Alliance RRG (“LSA”) and the policyholder have an insurer/insured relationship by virtue of a professional liability policy issued by LSA to the policyholder (hereinafter “Insurance Policy”). LSA and the policyholder are committed to complying with the Standards for Privacy and Security of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the Health Information Technology for Economic and Clinical Health Act (“HITECH”) and the revisions of 2013 made by the Omnibus Rule and all applicable state laws. Under the Privacy and Security Regulations, the policyholder is a “covered entity,” and, as defined by 45 CFR § 164.502(e) and 45 CFR § 164.504(e), LSA is a Business Associate of the policyholder. LSA must use and/or disclose Protected Health Information, as defined in 45 CFR § 164.501, in its performance of services under the Insurance Policy. LSA agrees to abide by the assurances, terms, and conditions contained herein in the performance of its obligations. This Agreement sets forth the manner in which Protected Health Information, that is provided to, or received by, LSA from the policyholder, or on behalf of the policyholder, will be handled.

Definitions

Catch-all definitions: The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

- (a) Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean LSA.
- (b) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean the policyholder.
- (c) HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- (d) Sensitive Personal Information (SPI). Texas Business and Commerce, Chapter 521, Unauthorized use of Identifying Information defines SPI more broadly than HIPAA Protected Health Information; an Individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
 - social security number;
 - driver's license number or government-issued identification number; or,
 - account number or credit or debit card number in combination with any required security code,

access code, or password that would permit access to an Individual's financial account; or, information that identifies an Individual and relates to:

- the physical or mental health or condition of the Individual;
- the provision of health care to the Individual; or,
- payment for the provision of health care to the Individual.

SECTION 1

Obligations and Activities of Business Associate

LSA agrees to:

- 1.1 Not Use or Disclose Protected Health Information Unless Permitted.** LSA may receive from policyholder health information protected under state or federal law, including Protected Health Information and/or electronic Protected Health Information (hereinafter both shall be referred to as Protected Health Information). LSA agrees not to use, or further disclose, Protected Health Information other than as permitted or required by the Agreement or as required or allowed by law.
- 1.2 Use Appropriate Safeguards.** LSA agrees to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to Protected Health Information, to prevent use or Disclosure of Protected Health Information other than provided for by the Agreement or as otherwise required or allowed by law. LSA acknowledges that the HITECH Act and the HIPAA Omnibus Rule requires LSA to comply with the security provisions in 45 CFR § 164.308, 164.312 and 164.316 as well as all additional security provisions of the HITECH Act as if LSA were a Covered Entity.
- 1.3 Report Inappropriate Disclosures of Protected Health Information.** LSA agrees to report to policyholder any use or Disclosure of Protected Health Information not permitted by this Agreement or by law of which it becomes aware. LSA will comply with Section 13402 of the HITECH Act with respect to timeliness, method and content of the report. LSA agrees to notify the Covered Entity within 5 business days of LSA's knowledge of any use or Disclosure of the Protected Health Information not permitted by this Agreement or by law.
- 1.4 Compliance of Agents.** LSA agrees, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), to require any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate to agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.
- 1.5 Access.** LSA agrees to make available Protected Health Information in a Designated Record Set to "Covered Entity", as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524. To the extent that LSA maintains an original Designated Record Set, as such term is defined in 45 CFR § 164.501, or a part thereof, LSA agrees to provide access to the policyholder to Protected Health Information in the original Designated Record Set, during normal business hours, provided the policyholder delivers prior written notice to LSA, at least five business days in advance, requesting such access but only to the extent required by 45 CFR § 164.524.
- 1.6 Amendments.** To the extent LSA maintains an original Designated Record Set, or a part thereof, LSA agrees to make Protected Health Information available for amendment to the policyholder and to incorporate any amendment(s) to Protected Health Information in the original Designated Record Set that the policyholder directs, pursuant to 45 CFR § 164.526. Any requests for amendment to the original Designated Record Set should be made through the Covered Entity and their existing policy and procedure or the amendment process.
- 1.7 Disclosure of Practices, Books, and Records.** Unless otherwise protected from discovery or Disclosure by

law or unless otherwise prohibited from discovery or Disclosure by law, LSA agrees to make internal practices, books, and records available to the policyholder or to the Secretary of the Department of Health and Human Services (hereinafter referred to as “Secretary”), for purposes of the Secretary determining the policyholder’s compliance with the Privacy Regulations but only to the extent such access is related to the use and Disclosure of Protected Health Information received from the policyholder, or created or received by LSA on behalf of the policyholder. LSA shall have a reasonable time within which to comply with such requests and, in no case shall access be required in less than five business days after LSA is in receipt of such request.

- 1.8 Accounting.** Pursuant to 45 CFR § 164.528, as amended by Section 13405 (c) of the HITECH Act and any related regulations or guidelines, LSA agrees to maintain sufficient documentation of Disclosures of Protected Health Information and information related to such Disclosures as would be required for the policyholder to respond to a request by an Individual for an accounting of Disclosures of Protected Health Information.
- 1.9 Release of Documentation of Disclosure.** LSA agrees to provide to the policyholder, or others as Required by Law, information collected in accordance with Section 1.8 of this Agreement, to permit the policyholder to respond to a request by an Individual for an accounting of Disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

SECTION 2

Permitted Uses and Disclosures by Business Associates

- 2.1 Use of Protected Health Information for Specified Purposes.** Except as otherwise Required by Law, LSA shall use Protected Health Information in compliance with 45 CFR § 164.504e. Under the Insurance Policy, LSA provides the policyholder with insurance products and services (hereinafter “Services”) that involve the use and Disclosure of Protected Health Information as defined by the Privacy Regulations. These Services may include, among others, the provision of professional liability insurance; receiving and evaluating incidents, claims, and lawsuits; quality assessment; quality improvement; loss prevention tools; outcomes evaluation; protocol and clinical guidelines development; reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance; conducting training programs to improve the skills of health care practitioners and providers; credentialing, conducting or arranging for medical review; arranging for legal services; conducting, or arranging for audits to improve compliance; resolution of internal grievances; placing stop-loss and excess of loss insurance, and other functions necessary to perform these Services. Except as otherwise specified herein, LSA may make any uses of Protected Health Information necessary to perform its obligations under this Agreement and under the Insurance Policy, if such use of Protected Health Information would not violate the Privacy Regulations. Moreover, LSA may disclose Protected Health Information for the purposes authorized by this Agreement: (1) to its employees, Subcontractors, and agents, in accordance with paragraphs 2.2 through 2.4 of this Section below; or (2) as otherwise permitted by the terms of this Agreement. All other uses not authorized by this Agreement are prohibited. LSA may use or disclose Protected Health Information that has been fully de-identified as Required by Law.
- 2.2 Use of Protected Health Information for Business Associate Management and Administration.** LSA may use Protected Health Information for the proper management and administration of LSA or to carry out the legal responsibilities of LSA.
- 2.3 Disclosure Required by Law or With Reasonable Assurances.** LSA may disclose Protected Health Information for proper management and administration and to carry out its legal responsibilities, provided that Disclosures are Required by Law, or provided that LSA obtains the following reasonable assurances from the person or entity to whom the Protected Health Information is disclosed: 1) the Protected Health Information will remain confidential; 2) the Protected Health Information will be used or further disclosed

only as required by law or for the purposes for which it was disclosed; and, 3) the person or entity will notify LSA of any instances of which the person or entity is aware in which the confidentiality of the information has been breached. In compliance with Section 13405(b) of the HITECH act, LSA will only disclose the Minimum Necessary to accomplish the intended purpose of the Disclosure and, if applicable, to the limited data set as defined in 45 CFR § 164.514(e)(2).

- 2.4 Data Aggregation Services.** If necessary to provide services related to a policyholder's Health Care Operations, LSA may use Protected Health Information to provide Data Aggregation services to the policyholder as permitted by 45 CFR § 164.504(e)(2)(i)(B).
- 2.5 Disclosure to Report Violations of Law.** LSA may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

SECTION 3

Obligations of and Permissible Requests by Policyholder

- 3.1 Notification of Limitation(s).** The policyholder shall notify LSA of any limitation(s) in its Notice of Privacy Practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect LSA's use or Disclosure of Protected Health Information.
- 3.2 Notification of Changes or Revocation.** The policyholder shall notify LSA of any changes in, or revocation of, permission to use or disclose Protected Health Information, to the extent that such changes may affect LSA's use or Disclosure of Protected Health Information.
- 3.3 Notification of Restriction.** The policyholder shall notify LSA of any restriction to the use or Disclosure of Protected Health Information that the policyholder has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect LSA's use or Disclosure of Protected Health Information.
- 3.4 Permissible Requests.** The policyholder shall not request LSA to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Regulations if done by the policyholder. This provision does not apply to LSA's use or Disclosure of Protected Health Information for Data Aggregation or management and administrative activities as is otherwise permitted by this Agreement.

SECTION 4

Term and Termination of Agreement

- 4.1 Term.** The Term of this Agreement shall be effective beginning September 23, 2013 and shall terminate when all of the Protected Health Information provided by the policyholder to LSA, or created or received by LSA on behalf of the policyholder, is destroyed. This Agreement shall supersede any existing Business Associate Agreements issued in accordance with HIPAA.
- 4.2 Termination for Cause.** Upon the policyholder's knowledge of a material Breach by LSA of this Agreement, the policyholder shall either:
- 1.) Provide an opportunity for LSA to cure the Breach or end the violation within a reasonable period of time. If LSA does not cure the Breach or end the violation within the reasonable period of time specified by the policyholder, the policyholder shall terminate this Agreement and the underlying Insurance Policy; or
 - 2.) Immediately terminate this Agreement and the underlying Insurance Policy if LSA has breached a material term of this Agreement and cure is not possible;

4.3 Effect of Termination.

- 1.) Due to the infeasibility of returning Protected Health Information to the policyholder, upon termination of this Agreement and/or the underlying Insurance Policy, for any reason, LSA shall securely retain and/or destroy all Protected Health Information received from the policyholder, or created or received by LSA on behalf of the policyholder in accordance with LSA's policies for retention and destruction of Protected Health Information.
- 2.) LSA shall limit further uses and Disclosures to those purposes that make the return of the Protected Health Information infeasible. LSA shall extend the protections of this Agreement to such Protected Health Information for so long as LSA maintains such Protected Health Information.

SECTION 5 Miscellaneous Provisions

- 5.1 Regulatory References.** A reference in this Agreement to a section in the Privacy Regulations means the section as in effect or as amended.
- 5.2 Amendment.** LSA and the policyholder agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the policyholder to comply with the requirements of HIPAA Rules and any other applicable law.
- 5.3 Survival.** The respective rights and obligations of LSA under Section 4.3 of this Agreement shall survive the termination of this Agreement.
- 5.4 Interpretation.** Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules



Debbie Giese
Vice President Underwriting
Lone Star Alliance RRG