HIPAA BUSINESS ASSOCIATE AGREEMENT

If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in its Customer Personal Data uploaded through the Rubrik Service ("**Services**"), this HIPAA Business Associate Agreement ("**BAA**") is incorporated upon execution of the Rubrik Services Agreement (the "**Agreement**") that incorporates the Rubrik Data Processing Addendum. If there is any conflict between a provision in this BAA and a provision in the Agreement, this BAA will control.

WHEREAS, Customer Personal Data may contain Protected Health Information ("**PHI**"), as defined in this BAA, thereby creating a business associate relationship between Customer and Rubrik, and such relationship shall only arise to the extent Customer actually discloses PHI to Rubrik; and,

WHEREAS, both parties intend to protect the privacy and provide for the security of PHI disclosed to Rubrik pursuant to the Agreement in compliance with: (i) the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"); (ii) the Health Information Technology for Economic and Clinical Health Act ("**HITECH**"); and (iii) regulations promulgated thereunder by the U.S. Department of Health and Human Services, including the HIPAA Standard Transactions and Code Sets Regulations and the HIPAA Omnibus Final Rule (the "**HIPAA Final Rule**"), which amended the HIPAA Standards for Privacy of Individually Identifiable Health Information (the "**Privacy Rule**") and the HIPAA Security Standards Regulations (the "**Security Rule**") pursuant to HITECH, extending certain HIPAA obligations to business associates and their subcontractors (all of the foregoing regulations collectively referred to herein as "**HIPAA**"). The parties hereby enter into this mutually acceptable BAA as necessary to so comply.

NOW, THEREFORE, for and in consideration of the foregoing obligations and for other good and valuable consideration of the parties set forth in the Agreement and this BAA and intending to be legally bound hereby, the parties agree as follows:

1. DEFINITIONS

1.1 **Defined Terms**. The terms set forth below shall be defined in this BAA as follows:

a. "**Electronic Protected Health Information**" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R § 160.103.

b. "**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R Part 160 and Part 164, Subparts A and E.

c. "**Protected Health Information**" or "**PHI**" shall have the same meaning as the term "protected health information" in 45 C.F.R § 160.103, limited to the information received or created by Rubrik from or on behalf of Customer.

d. "**Required By Law**" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103

e. "**Secretary**" means the Secretary of the Department of Health and Human Services or his designee.

f. "**Security Incident**" shall have the same meaning as the term "security incident" in 45 C.F.R. § 164.304.

g. "**Security Rule**" means the Security Standards and Implementation Specifications at 45 CFR §§ 164.306, 164.308, 164.310, 164.312, and 164.316.

h. "**Unsecured Protected Health Information**" shall have the same meaning as the term "unsecured protected health information" in 45 C.F.R. § 164.402.

1.2 **General**. The following terms used in this BAA shall have the same meaning as those terms in HIPAA: Breach, Business Associate, Covered Entity, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Subcontractor, and Use. Regulatory citations in this BAA are to the C.F.R., as interpreted by HHS, for so long as such regulations remain in effect. Unless otherwise specified in this BAA, all terms not otherwise defined in this BAA shall have the meanings established under 45 C.F.R. parts 160 through 164.

2. PERMITTED USES AND DISCLOSURES OF PHI

2.1 **Use and Disclosure**. Rubrik shall not use or further disclose PHI other than as permitted or required by this BAA or as Required By Law. PHI for purposes of this BAA shall be limited to PHI created, received or maintained by Rubrik from or on behalf of Customer.

2.2 **Services**. Except as otherwise limited by this BAA, Rubrik may use or disclose the PHI necessary to provide the Services for, or on behalf of Customer as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by the Customer. To the extent that Rubrik is carrying out any of Customer's obligations under the Privacy Rule pursuant to the terms of the Agreement or this BAA, Rubrik shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation(s).

2.3 **Subcontractors**. Rubrik shall ensure that any agents, including Subcontractors, to whom it provides PHI received from (or created or received by Rubrik on behalf of) Customer agree to the same restrictions and conditions that apply to Rubrik with respect to such PHI in this BAA.

2.4 **De-identification**. If applicable as part of the services, Rubrik will de-identify any and all PHI, provided that the de-identification conforms to the requirements of 45 C.F.R. § 164.514(b). De-identified information does not constitute PHI and is not subject to the terms of this BAA.

3. RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PHI

3.1 **Responsibilities of Rubrik**. Regarding any PHI that may be disclosed to Rubrik, including any use and/or disclosure of PHI and the privacy and security of PHI, Rubrik hereby agrees as follows:

a. **Appropriate Safeguards**. Rubrik will use reasonable and appropriate safeguards and shall comply with the Security Rule with respect to Electronic PHI, to prevent the unauthorized use and disclosure of PHI other than as provided by the Agreement and this BAA.

b. **Sanctions**. Rubrik shall establish and implement procedures to sanction its employees who violate the provisions of this BAA.

c. **Mitigation**. Rubrik shall mitigate, to extent practicable, any harmful effects known to Rubrik of a use or disclosure of PHI that is not permitted by this BAA.

d. **Reporting**.

(i) Rubrik shall report to Customer any Security Incident, without unreasonable delay, and in any event no more than seventy-two (72) hours following discovery; provided, however, that the parties acknowledge and agree that this Section constitutes notice by Rubrik to Customer of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which notice to Customer by Rubrik shall be required only upon request. "**Unsuccessful Security Incidents**" shall include, but not be limited to, pings and other broadcast attacks on Rubrik's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in a Breach. Rubrik's notification to Customer of a Breach shall include, to the extent known at the time and : (i) the identification of each individual whose Unsecured PHI has been, or

is reasonably believed by Rubrik to have been, accessed, acquired or disclosed during the Breach; (ii) a general description of the incident (including who the threat actor is or is suspected to be, the general type of attack, if the incident is contained, a general timeline of the attack and Rubrik's operability); and (iii) any particulars regarding the Breach that Customer would need to include in its notification, as such particulars are identified in 45 C.F.R. § 164.404.

(ii) Rubrik shall investigate the Security Incident in cooperation with Customer. At the time of the initial report (if known), or without unreasonable delay after the initial report (if unknown at the time of the original report), Rubrik shall report the following to the extent known and subsequently as such information becomes available: identity of each individual whose unsecured PHI has been or is reasonably believed to have been, accessed, acquired or disclosed, the date of the disclosure, a brief description of the PHI disclosed, and brief description what happened regarding the disclosure, and any other information required in order for the Customer to fulfill its breach notification obligations under the HIPAA Regulations.

(iii) Rubrik shall mitigate to the extent practicable, any harmful effect that is known to Rubrik of a use or disclosure of PHI by Rubrik in violation of this Agreement. Upon request, each party shall promptly provide the other party with information relating to its discovery, investigation and mitigation activities associated with a Breach that affects the other party.

e. **Access to Internal Practices**. At the request of, and at the time and in the manner designated by Customer or the Secretary, Rubrik shall make its internal practices, books and records (including policies and procedures) relating to the use and/or disclosure of PHI available to (i) the Customer, and its representatives for the purpose of assessing Rubrik's compliance with this BAA and/or the Customer's compliance with the Privacy Rule, or (ii) to the Secretary for purposes of the Secretary determining Customer's and/or Rubrik's compliance with the Privacy Rule.

f. **Access to PHI**. If applicable as part of the Services for Rubrik to maintain a designated record set, Rubrik shall make an individual's PHI in a designated record set available for inspection and copying in accordance with 45 C.F.R. § 164.524. Further, within ten (10) days of Rubrik's receipt of Customer's request, Rubrik shall provide Customer with the PHI requested by an individual pursuant to 45 C.F.R. § 164.524, to the extent possible based upon the nature of the Services. Alternatively, at Customer's request, Rubrik shall cooperate with Customer to provide an individual with access to his/her PHI in the time and manner designated by the Customer.

g. **Amendments to PHI**. Rubrik shall make an individual's PHI available for amendment and shall incorporate any amendments to the PHI in accordance with 45 C.F.R. § 164.526, to the extent possible based upon the nature of the Services. Further, within ten (10) days of Rubrik's receipt of the Customer's request, Rubrik shall provide Customer with the PHI that an individual seeks to amend pursuant to 45 C.F.R. § 164.526, to the extent possible based upon the nature of the Services.

h. **Accounting of Disclosures**. Rubrik shall make available the information required to provide an accounting of disclosures to an individual pursuant to 45 C.F.R. § 164.528, to the extent possible based upon the nature of the Services. Further, at Customer's request, within ten (10) days of Rubrik's receipt of Customer's request, Rubrik shall provide Customer with such information. To fulfill this obligation Rubrik agrees to document those disclosures of PHI and related information that would be necessary for the Customer to respond to an individual's request for an accounting of disclosures.

i. **Restrictions/Alternatives**. Rubrik shall abide by any arrangements that Customer has made with an individual regarding restricting the use or disclosure of the individual's PHI or providing the individual with confidential communications of PHI by alternative means or at an alternative location pursuant to 45 C.F.R. § 164.522, to the extent possible based upon the nature of the Services.

j. **Minimum Necessary**. Rubrik (and its agents or Subcontractors) shall request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or

disclosure in accordance with 45 C.F.R. § 164.502(b). Rubrik shall implement access controls that enable authorized users to access the minimum necessary PHI needed to perform job functions. Rights and/or privileges should be granted to authorized users based on a set of access rules that Rubrik is required to implement as part of 45 C.F.R. § 164.308(a)(3) and 45 C.F.R.§ 164.308(a)(4).

3.2 **Responsibilities of Customer**.

a. **Consent**. Customer agrees to obtain in writing any individual's consent, authorization, and other permissions that may be necessary or required by applicable laws in order to transfer or disclose the PHI to Rubrik.

b. **Notification**. Customer shall promptly notify Rubrik of any changes or limitation(s) in the notice of privacy practices of Customer under 45 CFR 164.520, to the extent that such limitation may affect Rubrik's use or disclosure of PHI.

c. **Changes**. Customer shall promptly notify Rubrik of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Rubrik's use or disclosure of PHI.

d. **Restrictions**. Customer shall promptly notify Rubrik of any restriction on the use or disclosure of PHI that Customer has agreed to or is required to abide by under 45 C.F.R. §164.522, to the extent that such restriction may affect Rubrik's use or disclosure of PHI.

e. **Requests**. Customer acknowledges that the nature of the Service is such that Rubrik may need Customer's cooperation and assistance in order to make an individual's PHI available pursuant to 45 C.F.R. § 164.524. As such, Customer agrees to promptly notify Rubrik, in writing, of the PHI in Rubrik's custody that Customer seeks to make available to an individual and agree with Rubrik as to the time, manner, and form in which Rubrik shall make the PHI available.

f. **Disclosures**. Customer shall not request Rubrik to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Customer.

4. STANDARD TRANSACTIONS AND CODE SETS

If applicable as part of the Services, should Rubrik conduct, in whole or in part, Standard Transactions for or on behalf of Customer, Rubrik shall comply, and shall require any Subcontractor involved with the conduct of such Standard Transactions to comply, with each applicable requirement of 45 C.F.R. Part 162. Rubrik shall comply with the National Provider Identifier requirements, if and to the extent applicable. Rubrik shall provide to Customer any documentation of compliance with the Transaction Rule, which Customer may reasonably need, if any, pursuant to section 1104(b) of the Patient Protection and Affordable Care Act, as amended.

5. BUSINESS CONTINUITY

Pursuant to 45 C.F.R. § 164.308, Rubrik has established procedures relevant to the Services for securing and protecting PHI during a general disaster or disruption of critical business processes.

6. TERMS AND TERMINATION

6.1 **Term**. This BAA shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein. This BAA shall automatically expire or terminate without any further action of the parties upon the termination or expiration of the Agreement.

6.2 **Termination.** Notwithstanding anything in the Agreement to the contrary, if either party breaches its obligations under this BAA, in any form or manner, the other party may, in its sole discretion, immediately terminate this BAA or the applicable portion of the Agreement covering the affected Services, by giving written notice of the existence of the alleged breach and allowing the breaching party an opportunity to cure the alleged breach within thirty (30) calendar days.

6.3 **Effect of Termination**. Except as provided herein, upon expiration or termination of this BAA or the Agreement, Rubrik shall return or delete all PHI and not retain any copies of such PHI in any format, if it is feasible to do so, in accordance with the process set forth in the Agreement for the return or deletion of Customer Data, as that term is defined thereunder. If Rubrik determines that returning or deleting PHI is infeasible, Rubrik shall notify Customer in writing of the conditions that make return or deletion infeasible. Regarding any PHI that is not returned or deleted at the expiration or termination of this BAA, Rubrik shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or deletion infeasible, for as long as Rubrik maintain such PHI. In addition, Rubrik shall maintain the PHI in accordance with the records retention requirements under the Privacy Rule and Security Rule.

7. MISCELLANEOUS

7.1 **Entire Agreement**. This BAA is subject to the terms of the Agreement, and together, the BAA and Agreement constitute the entire agreement of the parties and supersede all prior or contemporaneous written or oral memoranda, arrangements, contracts or understandings between the parties hereto relating to the subject matter of this BAA.

7.2 **Regulatory References**. A reference in this BAA to a section in the Privacy Rule, the Standard Transactions and Code Sets Regulations, the Security Rule or the HIPAA Final Rule means the section as in effect or as amended, and for which compliance is required.

7.3 **Injunctive Relief.** If a party to this BAA, or such party's agents, employees or contractors, breaches or threatens to breach this BAA, then in addition to and without waiving any other available remedies, the affected party shall have the right to seek injunctive relief enjoining any such breach or threatened breach, it being acknowledged that legal remedies are inadequate and that the actions or inactions of the other party at issue may cause irreparable harm.

7.4 **Survival**. The provisions of this BAA shall survive the expiration or any termination of the term of the Agreement to the extent that Rubrik continues to maintain PHI. Further, after expiration or termination of this BAA, those provisions in this BAA that provide for survival, or which due to their nature reasonably should be deemed to survive, beyond expiration or termination, shall survive indefinitely.

7.5 **Interpretation**. Any ambiguity in this BAA shall be resolved to permit compliance with the Privacy Rule, the Standard Transactions and Code Sets Regulations, the Security Rule and HIPAA Final Rule.

7.6 **Amendments; Waiver**. This BAA may not be modified, and no provision hereof shall be waived or amended, except in a writing duly signed by authorized representatives of the parties. The parties agree to take such action necessary to amend this BAA from time to time as is necessary for compliance with the requirements of or conform to any changes in the Privacy Rule, Standard Transactions and Code Sets Regulations, the Security Rule or the HIPAA Final Rule. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

7.7 **No Third-Party Beneficiaries**. Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assigns of the parties, any rights, remedies, obligations, or liabilities whatsoever.

7.8 **Disputes**. Subject to and to the extent allowable by law, if any controversy, dispute or claim arises between the parties with respect to this BAA, the parties shall comply with any relevant provision of the Agreement pertaining to disputes, including without limitation the processes and obligations identified therein.