Business Associate Agreement

While Commvault does not have visibility into the nature of Customer Data due to encryption, we understand our Customers may be subject to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act Title XIII of the American Recovery and Reinvestment Act, 2009 and regulations promulgated thereunder from time to time ("HIPAA"). To the extent Customer chooses to backup protected health information ("PHI") within the SaaS Solution, this Business Associate Agreement (the "BAA") forms part of the Master Terms and Conditions, or other agreement between Commvault and Customer for the purchase of Commvault's products and services. Any terms not defined have the same definition ascribed to them in the Master Terms and Conditions or HIPAA. Customer enters into this BAA as the Covered Entity. To execute this BAA, Customer should complete Customer's information and return the fully executed BAA to contracts@commvault.com.

1. **Obligations and Activities of Commvault.** In connection with the obligations of a Business Associate, Commvault agrees to: (a) not use or disclose PHI other than to provision the SaaS Solution, or as permitted or required by law or this BAA; (b) use reasonable and appropriate privacy and security safeguards to prevent use or disclosure of PHI as provided for by this BAA and consistent with the requirements of the Security Rule set forth at Subpart C of 45 CFR Part 164 with respect to PHI as determined by Commvault; and (c) report to Customer any use or disclosure of PHI not provided for in connection with the provision of the SaaS Solution or this BAA, of which it becomes aware, including breaches of unsecured PHI as required by 45 CFR 164.410; provided that notice is hereby deemed given for "Unsuccessful Security Incidents." defined as a security incident that does not result in the unauthorized access, use, disclosure, modification or destruction of PHI, or interference with system operations in an information system. This notice shall satisfy any notices required of Commvault to Customer of the ongoing existence and occurrence of Unsuccessful Security Incidents, for which no additional notice to Customer shall be given or required. Notification of a breach of unsecured PHI under 45 CFR 164.410 will be made without unreasonable delay, but in no event more than seventy-two (72) hours after Commvault's discovery thereof and will be delivered to Customer by means selected by Commvault, including via email (a "Notice"). Commvault's obligation of notification under this section shall not be construed as an acknowledgment by Commvault of any fault or liability with respect to any use or disclosure of PHI, or security incident or breach related thereto. Notice will include a description of the incident and the type of unsecured PHI involved. If applicable, Commvault shall ensure that, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), any of its subcontractors that create, receive, maintain, or transmit Customer's PHI on behalf of Commvault comply with restrictions, conditions, and requirements at least as stringent as those that apply to Commvault with respect to PHI. If Commvault maintains PHI in a Designated Record Set, upon Customer's request, Commvault shall provide Customer with access to the same for amendment. Commvault shall maintain and make available an accounting of disclosures (if any) to the Customer as necessary to satisfy Customer's obligations. To the extent Commvault is to carry out one or more of Customer's obligation(s) under Subpart E of 45 CFR Part 164, Commvault shall comply with the requirements of Subpart E that apply to the Customer in the performance of such obligations and make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary, for purposes of determining Customer's compliance with the HIPAA, subject to attorney-client and other applicable legal privileges.

2. **Permitted Uses and Disclosures by Commvault.** Commvault will use or disclose only the minimum necessary amount of PHI as set forth in this BAA or as required by law. Commvault shall not use or disclose PHI in any manner that would violate HIPAA if done by Customer. Commvault may use and disclose PHI for the proper management and administration of the SaaS Solution or to carry out Commvault's legal responsibilities, provided, the disclosures are required by law, or Commvault obtains reasonable assurances from the recipient of the information that any PHI will remain confidential, be used or further disclosed only as required by law or for the purposes for which it was disclosed to them, and the recipient shall be required to notify Commvault of any instances of which it is aware in which the confidentiality of the PHI has been breached. Commvault shall maintain an accounting of any disclosures of PHI in accordance with 45 CFR § 164.528.

3. **Provisions for Covered Entity to Inform Commvault of Privacy Practices and Restrictions.** To the extent it may affect Commvault's use or disclosure of PHI, Customer shall notify Commvault of: (i) any limitations in the notice of privacy practices of Customer under 45 CFR 164.520, (ii) any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, and (iii) any restriction on the use or disclosure of PHI that Customer has agreed to or is required to abide by under 45 CFR 164.522. Customer shall implement appropriate privacy and security safeguards to protect its PHI in compliance with HIPAA, and to protect its Customer Account details from unauthorized access. It is Customer's responsibility to ensure Customer has the appropriate business associate agreements in place. If Customer believes there has been unauthorized access to its Customer Account or Customer Data, Customer must immediately notify legal@commvault.com. In addition, Customer shall indemnify, defend and hold Commvault harmless from and against any damages and costs arising from or relating to Customer's failure to implement appropriate privacy and security safeguards to protect its Customer Account and Customer Data.

4. **Term and Termination.** This BAA is coterminous with the Terms and any applicable purchase order. Upon either party's knowledge of a breach or violation of this BAA by the other party, the non-breaching party will require the breaching party to take reasonable steps to cure the breach or end the violation. If the breaching party does not cure the breach or end the violation within the time specified by the non-breaching party, or if no cure or end of violation is possible, the non-breaching party may immediately terminate this BAA upon written notice to the breaching party. If the Secretary provides guidance, clarification or interpretation of HIPAA or there is a change in HIPAA that the relationship between Commvault and Customer is not considered a Business Associate relationship, this BAA shall terminate and be null and void. Following expiration, cancellation or termination of the Terms and any applicable purchase order, Commvault and its subcontractors will destroy or return upon request all Customer Data which may include PHI within a reasonable amount of time unless such destruction or return is not commercially practical. Commvault shall continue to treat PHI as set forth herein for the duration of its possession thereof.

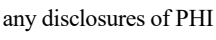
5. **Miscellaneous.** A reference in this BAA to a section in HIPAA means the section as in effect or as amended. Any ambiguity in this BAA shall be interpreted to permit compliance with HIPAA. The parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for compliance with the requirements of HIPAA. Except as expressly provided for in the Privacy Rule, there are no third-party beneficiaries to this BAA and Commvault's obligations are to Customer only. This BAA shall be governed by and construed in accordance with federal law as it pertains to the subject matter.

CUSTOMER NAME

_____

Name:
Email:
Date:

COMMVAULT



Name: Meg Cavanaugh
Title: SVP – Deputy General Counsel