HIPAA Business Associate Addendum for the Standard Contract for AWS Marketplace

This HIPAA Business Associate Addendum (this “BAA”) is part of the Standard Contract for AWS Marketplace (the “Standard Contract”) between Buyer and Licensor and governs the creation, receipt, maintenance, or transmission of Protected Health Information on behalf of the Covered Entity (the “Buyer”) by the Licensor as Business Associate (the “Supplier”). Each of the Standard Contract and/or the Data Subscription Agreement is a Standard Contract. Each Seller and each Licensor is a Supplier. This Addendum is not applicable if Supplier does not create, receive, maintain, or transmit Protected Health Information on behalf of Buyer or if Buyer is not subject to the Administrative Simplification of the Health Insurance Portability and Accountability Act of 1996, as amended, the Health Information Technology for Economic and Clinical Health Act of 2009, and their implementing regulations (collectively “HIPAA”) as a Covered Entity or Business Associate.

1. Definitions

1.1 All capitalized terms used but not otherwise defined in this BAA or the Standard Contract shall have the same meaning as those terms are defined by HIPAA.

1.2 “Individual” shall have the same meaning as the term “individual” in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.3 “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, and refer to individually identifiable information that is received, created, maintained, or transmitted by Supplier on behalf of Buyer.

2. Permitted Uses and Disclosures by Supplier

2.1 Except as otherwise limited in this BAA, Supplier may Use or Disclose Protected Health Information in its possession to perform functions, activities, or services for, or on behalf of, Buyer as specified in the Standard Contract consistent with Buyer’s minimum necessary policies and procedures, provided that such Use or Disclosure would not violate HIPAA if done by Buyer.

2.2 Except as otherwise limited in this BAA, Supplier may Use Protected Health Information for the proper management and administration of Supplier or to carry out the legal responsibilities of Supplier.

2.3 Except as otherwise limited in this BAA, Supplier may Disclose the Protected Health Information in its possession to a third party for the proper management and administration or to fulfill any legal responsibilities of Supplier, provided that:

2.3.1 The Disclosure is Required by Law; or

2.3.2 Supplier has received from the third party reasonable written assurances that: (1) the information will remain confidential and will be Used or further Disclosed only as
2.4 Supplier may not Use Protected Health Information to create de-identified Health Information in accordance with 45 C.F.R. § 164.514(b) for purposes unrelated to the Standard Contract without prior written approval of Buyer.

3. Obligations and Activities of Supplier

3.1 Supplier shall not Use or Disclose Protected Health Information other than as permitted or required by this BAA or as Required By Law.

3.2 Supplier agrees to use appropriate administrative, physical, and technical safeguards and comply, where applicable, with the Security Standards for Protection of Electronic Protected Health Information, 45 C.F.R. Part 164 Subpart C (the “Security Rule”) with respect to Electronic Protected Health Information, to prevent Use or Disclosure of the Protected Health Information other than as provided for by this BAA.

3.3 Supplier agrees to comply with the applicable requirements of the Security Rule.

3.4 Supplier agrees to mitigate, to the extent practicable, any harmful effect that is known to Supplier of a Use or Disclosure of Protected Health Information by Supplier in violation of the requirements of this BAA.

3.5 Supplier agrees to report to Buyer, without unreasonable delay and no later than within five (5) business days of discovery:

3.5.1 Any Use or Disclosure of Protected Health Information not provided for by this BAA, including Breaches of Unsecured Protected Health Information; and/or

3.5.2 Any Security Incident, provided that this Section shall hereby serve as notice, and no additional reporting shall be required, of any unsuccessful attempts at unauthorized Access, Use, Disclosure, modification, or destruction of information or unsuccessful interference with system operations in an information system.

3.6 For any Breach of Unsecured Protected Health Information of which it becomes aware, Supplier agrees to supplement the above report with the information required by 45 C.F.R. § 164.410 without unreasonable delay and in no case later than 30 calendar days after discovery of the Breach.

3.7 In accordance with 45 C.F.R.§ 164.502(e)(1)(ii) and 164.608(b)(2), Supplier agrees to ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on Supplier’s behalf agree in writing to: (a) the same restrictions and conditions that apply through this BAA to Supplier with respect to such Protected Health Information and meet HIPAA requirements, including complying with the applicable requirements of the Security Rule; and (b) comply with the requirements of the Security Rule that apply to a Business Associate. Supplier shall not allow any of its Subcontractors to create,
receive, maintain, or transmit Protected Health Information on Supplier’s behalf unless Supplier first has conducted reasonable due diligence of the Subcontractor and its information security and determined that its security is reasonable.

3.8 Supplier agrees to make its internal practices, books, and records relating to the Use and Disclosure of Protected Health Information received from, or created or received by Supplier on behalf of Buyer, available to the Secretary of the Department of Health and Human Services (“Secretary”) for the purposes of the Secretary determining compliance with HIPAA. Nothing in this Section shall be construed as a waiver of any legal privilege or of any protections for trade secrets or confidential commercial information.

3.9 Supplier, upon request by Buyer, will make Protected Health Information in a Designated Record Set available to Buyer or, at the request of Buyer, the Individual, within five (5) days of Buyer’s request, as necessary to allow Buyer to comply with its obligations to provide access to Individuals of their health information as required by 45 C.F.R. § 164.524. To the extent that Protected Health Information in a Designated Record Set is available to Buyer through access to the SaaS Service, then Supplier satisfies its obligations under this Section through the provision of the SaaS Service.

3.10 Supplier, upon request by Buyer, will make Protected Health Information in a Designated Record Set available to Buyer and will incorporate any amendments to such information as instructed by Buyer within ten (10) days of a request, as necessary to allow Buyer to comply with its amendment obligations as required by 45 C.F.R. § 164.526. To the extent that Buyer can amend Protected Health Information in a Designated Record Set through use of the SaaS Service, then Supplier satisfies its obligations under this Section through the provision of the SaaS Service.

3.11 Supplier will maintain and, upon request by Buyer, within ten (10) days provide Buyer with the information necessary for Buyer to provide an Individual with an accounting of Disclosures as required by 45 C.F.R. § 164.528.

3.12 To the extent that Supplier is to carry out one or more of Buyer’s obligations under the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 164 Subpart E (the “Privacy Rule”), including but not limited to the provision of a notice of privacy practices on behalf of Buyer, Supplier shall comply with the requirements of the Privacy Rule that apply to Buyer in the performance of such obligations.

4. Obligations of Buyer

4.1 In the event that Buyer is a Covered Entity, then Buyer shall notify Supplier of any limitation(s) in Buyer’s notice of privacy practices under 45 C.F.R. §164.520, to the extent that such limitation may affect Supplier’s use or disclosure of Protected Health Information. In the event that Buyer is purchasing the SaaS Services as a Business Associate of one or more Covered Entities, then Buyer shall notify Supplier of any applicable limitation(s) of a Covered Entity’s notice of privacy practices under 45 C.F.R. §164.520, to the extent that Buyer is aware of such limitation and such limitations may affect Supplier’s use or disclosure of Protected Health Information.
4.2 Buyer shall notify Supplier of any changes in, or revocation of, the permission by an Individual to use or disclose his or her Protected Health Information, to the extent that Buyer is aware of such changes and such changes may affect Supplier’s use or disclosure of Protected Health Information.

4.3 Buyer shall notify Supplier of any restriction on the use or disclosure of Protected Health Information under 45 C.F.R. §164.522, to the extent that Buyer is aware of such restriction and such restriction may affect Supplier’s use or disclosure of Protected Health Information.

4.4 Buyer shall not knowingly request or cause Supplier to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Buyer, except as otherwise set forth in Sections 2.2 and 2.3 of this BAA.

5. Term and Termination

5.1 This BAA shall remain in full force and effect through the term of the Standard Contract.

5.2 For purposes of the termination provisions of the Standard Contract at Section 10.2 of the Standard Contract, a breach of this BAA shall constitute a breach of the Standard Contract.

5.3 Except as provided in Section 5.4 of this BAA, upon termination of the Standard Contract for any reason, Supplier shall return or destroy all Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of Subcontractors of Supplier. Supplier shall retain no copies of the Protected Health Information.

5.4 In the event that Supplier determines that returning or destroying the Protected Health Information is infeasible, and to the extent the Supplier retains any knowledge of the Protected Health Information, then Supplier shall extend the protections of this BAA to such Protected Health Information and limit further Uses and Disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for as long as Supplier maintains such Protected Health Information. This Section shall survive the termination of this BAA for any reason.

6. Miscellaneous

6.1 This BAA modifies and supplements the terms and conditions of the Standard Contract and shall be deemed a part of the Standard Contract. Any ambiguity in this BAA shall be resolved to permit the parties to comply with HIPAA and other applicable laws. In the event any provision of the Standard Contract conflicts or is inconsistent with this BAA, then this BAA shall control.

6.2 Nothing in this BAA shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
6.3 Except as specifically required to implement the purposes of this BAA, or to the extent inconsistent with this BAA, all other terms of the Standard Contract shall remain in force and effect.