BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("**BAA**") is entered into between Databricks, Inc., the parent company of Neon, LLC ("**Databricks**") and the customer agreeing to the terms below ("**Customer**") and supplements, amends, and is incorporated into the Product Specific Schedule (Neon) at https://neon.com/platform-terms, or, other agreement executed between you and Databricks governing your use of the Platform Services (in either case, the "**Agreement**").

1. **Definitions.** Capitalized terms used but not defined in this BAA will have the meaning given to them in the Agreement or HIPAA.

   1.1. "**Breach**" has the definition given to it under HIPAA. A Breach will not include an acquisition, access, use, or disclosure of PHI that Databricks has determined in accordance with 45. C.F.R. § 164.402 that there is a low probability that PHI has been compromised.

   1.2. "**Covered Services**" means the Platform Services.

   1.3. "**HIPAA**" means, collectively, the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, and their implementing and amending regulations.

   1.4. "**Security Breach**" means any Breach of Unsecured PHI or Security Incident that Databricks becomes aware of.

2. **Applicability.** This BAA applies to Covered Services to the extent Customer is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI via a Covered Service and to the extent Databricks, as a result, is deemed to be acting as a Business Associate or Subcontractor of a Business Associate under HIPAA. Customer agrees that it will not make PHI available to Databricks personnel outside the Covered Services.

3. **Use and Disclosure of PHI.**

   3.1. Databricks may use and disclose PHI only as permitted by this BAA, required by the Agreement, or as required by law.

   3.2. Databricks may use and disclose PHI for the proper management and administration of Databricks and to carry out its legal responsibilities, provided that any disclosure of PHI for such purposes may only occur if (i) required by applicable law, or (ii) Databricks obtains written reasonable assurances from the recipient to which PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Databricks will be notified of any Security Breach reportable to Customer.

   3.3. Databricks has no obligations under this BAA with respect to PHI that Customer creates, receives, maintains, or transmits outside of its Covered Services or in breach of the Agreement or this BAA, and, for clarity, this BAA will not apply to any such PHI.

   3.4. Except as requested by Customer in accordance with the Agreement, Databricks will not de-identify PHI for any purpose and/or distribute statistical analyses and reports utilizing aggregated data derived from PHI from Customer.

4. **Customer Obligations.**

   4.1. Customer is solely responsible for appropriately configuring and using the Covered Services in accordance with the Agreement and ensuring that its use of the Covered Services complies with HIPAA.

   4.2. Customer will not request that Databricks use or disclose PHI in any manner that would not be permissible under the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 164 Subpart E, if done by Customer, unless expressly permitted under HIPAA for a Business Associate.

   4.3. Customer is responsible for obtaining any necessary consents, authorizations, and other permissions required under HIPAA or other applicable law prior to uploading PHI to its Covered Services. If there are any changes in, or revocation of, such consents, authorizations, or permissions, Customer is responsible for managing its use of its Covered Services accordingly to update or delete such PHI in accordance with any resulting changes or revocations.

5. **Appropriate Safeguards.** Databricks will, with respect to the Covered Services, use commercially reasonable and appropriate administrative, physical, and technical safeguards and comply, where applicable, with the Security Standards for Protection of Electronic Protected Health Information required by 45 C.F.R. Part 164 Subpart C.

6. **Reporting.**

6.1. Databricks agrees to promptly, in no greater than five (5) business days, report to Customer any Security Breach of which Databricks becomes aware, provided that this section hereby serves as notice, and no additional notice shall be required, of any unsuccessful attempts at unauthorized access, use, disclosure, modification or destruction of information, or interference with the general operation of Databricks information systems and the Covered Services.

6.2. For any Security Breach, Databricks agrees to supplement the above notice with the information required by 45 C.F.R. § 164.410 without unreasonable delay and in no case later than sixty (60) calendar days after discovery by Databricks.

6.3. Databricks agrees to mitigate, to the extent commercially practicable, any harmful effects of a Security Breach caused by Databricks.

7. **Subcontractors.** Databricks will take appropriate measures to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Databricks are bound by restrictions and conditions that provide the same material level of protection for PHI as this BAA, and agree to implement reasonable and appropriate safeguards to protect PHI.

8. **Access and Amendment.** Customer acknowledges and agrees that Customer is solely responsible for PHI maintained by Customer within its Covered Services, including whether such PHI is maintained in a Designated Record Set. Databricks will make PHI available to Customer so Customer can fulfill its obligations with respect to Individuals' rights of access and amendment, but will have no other obligations to Customer with respect to Designated Record Sets, including rights of access or amendment of PHI as required by 45 C.F.R. § 164.524 and 45. C.F.R § 164.526.

9. **Accounting of Disclosures.** Databricks will, as and to the extent required of a Business Associate under HIPAA, maintain and, upon request by Customer, provide Customer with the information necessary for Customer to provide an Individual with an accounting of Disclosures as required by 45. C.F.R § 164.528.

10. **Access to Records.** To the extent required by applicable law, Databricks agrees to make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Databricks on behalf of Customer, available to the Secretary of the Department of Health and Human Services for the purposes of determining Customer's compliance with HIPAA. Nothing in this section shall be construed as a waiver of any legal privilege or any protections for trade secrets or confidential commercial information.

11. **Term and Termination.**

11.1. This BAA will terminate on the earlier of (i) permitted termination in accordance with Section 11.2 below, or (ii) the expiration or termination of the Agreement.

11.2. Upon either party's knowledge of a material breach of this BAA by the other party, the non-breaching party may terminate this BAA: (i) immediately if a cure is not reasonably possible, or (ii) if a cure is reasonably possible, after the non-breaching party has provided notice of at least thirty (30) calendar days and the breach is not cured within the 30-day period.

12. **Effect of Termination.**

12.1. If this BAA is terminated earlier than the Agreement, Customer may continue to use the Covered Services in accordance with the Agreement but must delete any PHI it maintains in any Covered Services and cease to further create, receive, maintain, or transmit PHI to Databricks.

12.2. Upon termination of this BAA, Business Associate shall return or destroy all PHI, provided that, in the event that Databricks determines that returning or destroying the PHI obtained by Databricks is infeasible, then Databricks will 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 destruction infeasible, for as long as Databricks maintains such PHI. This Section shall survive termination of this BAA.