**PALANTIR BUSINESS ASSOCIATE AGREEMENT ("BAA")**

The customer agreeing to the terms of this BAA ("**Customer**") and Palantir Technologies Inc., a Delaware corporation with its principal place of business located at 1200 17th Street, Floor 15, Denver, CO 80202 ("**Palantir**"; each of Customer and Palantir a "**Party**" and collectively the "**Parties**"), have entered into an agreement (such as the Palantir Terms of Service and Order Form) governing Customer's use of Palantir Technology, including the Service, and the provision of related Professional Services to Customer by Palantir, including any attachments, order forms, exhibits, and appendices thereto (collectively, the "**Agreement**"). This BAA supplements, is incorporated into, and forms part of the Agreement and establishes the rights and obligations of Palantir and Customer with respect to Palantir's use, disclosure, reception, access, creation, maintenance, and/or transmission of Protected Health Information on behalf of Customer in connection with Palantir's performance under the Agreement. Any capitalized terms used but not defined in this BAA shall have the meaning provided in the Agreement.

**WHEREAS**, Customer is a Covered Entity or Business Associate as those terms are defined in the federal regulations at 45 C.F.R. Parts 160 and 164, Subparts A and E (the "Privacy Rule");

**WHEREAS**, pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), the U.S. Department of Health and Human Services ("HHS") promulgated the Privacy Rule, the security standards at 45 C.F.R. Parts 160 and 164, Subparts A and C (the "Security Rule") and the breach notification standards at 45 C.F.R. Part 164, Subpart D (the "Breach Notification Rule") requiring certain individuals and entities subject to these standards to protect the privacy and security of certain individually identifiable health information, including electronic individually identifiable health information;

**WHEREAS**, the Parties are committed to complying with applicable provisions of the Privacy Rule, Security Rule, and Breach Notification Rule, as they may be revised or amended by HHS from time to time;

**NOW THEREFORE**, in consideration of the mutual promises set forth in this BAA and the Agreement, and other good and valuable consideration, the sufficiency and receipt of which are hereby acknowledged, the Parties agree as follows:

**1. DEFINITIONS**

All capitalized terms not otherwise defined in this BAA shall have the meanings set forth in the Agreement or in the regulations promulgated by HHS in accordance with HIPAA and HITECH, including the Privacy Rule and

Security Rule (collectively referred to hereinafter as the "Confidentiality Requirements"), as applicable. Specific definitions are as follows:

"Effective Date" shall be the same as the Effective Date of the Agreement.

"Electronic Protected Health Information" or "Electronic PHI" shall have the same meaning as the term "electronic protected health information" at 45 C.F.R. § 160.103. For purposes of this BAA, Electronic Protected Health Information and Electronic PHI shall mean only that electronic protected health information that Palantir uses, discloses, accesses, creates, receives, maintains, or transmits for or on behalf of Customer pursuant to the Agreement.

"Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" at 45 C.F.R. § 160.103. All references to PHI herein shall be construed to include Electronic PHI. For purposes of this BAA, PHI shall mean only that protected health information that Palantir uses, discloses, accesses, creates, receives, maintains, or transmits for or on behalf of Customer pursuant to the Agreement. For the avoidance of doubt, this PHI constitutes Customer Data.

**2. GENERAL PROVISIONS**

2.1 Effect. This BAA supersedes any prior business associate agreement between the Parties and those portions of any agreement between the Parties that involve the disclosure of PHI by Customer to Palantir. To the extent any conflict or inconsistency between this BAA and the terms and conditions of the Agreement as it relates to the subject matter herein the terms of this BAA shall prevail. In accordance with this BAA and the Agreement, Palantir may use, disclose, access, create, receive, maintain, or transmit PHI on behalf of Customer or as otherwise permitted in this BAA or Required by Law.

2.2 Amendment. This BAA may be modified or amended only by a written document executed by the authorized representatives of both Parties. The Parties may, upon mutual written agreement, amend this BAA to maintain consistency or compliance with any applicable state or federal law, policy, directive, regulation, or government-sponsored program requirement.

**3. SCOPE OF USE AND DISCLOSURE**

3.1 Non-Disclosure & Palantir's Operations. Palantir shall only use or disclose PHI as permitted by this BAA, to perform services as set forth in the Agreement, or as otherwise Required by Law. Except as limited in this BAA, in addition to any other uses and/or disclosures permitted or required by this BAA, Palantir may:

3.1.1 Use PHI as necessary for the proper management and administration of Palantir or to carry out its legal responsibilities.

3.1.2 Disclose PHI for the proper management and administration of Palantir or to carry out the legal responsibilities of Palantir; provided that: (i) such disclosures are Required by Law; or (ii) Palantir: (a) obtains reasonable assurances from any third party to whom the PHI is disclosed that the PHI will be held confidentially and used and disclosed only as Required by Law or for the purpose for which it was disclosed to the third party; and (b) requires the third party to agree to notify Palantir of any instances of which it is aware that the confidentiality of the information has been breached.

3.1.3 Use and disclose PHI for Data Aggregation services relating to the Health Care Operations of Customer, as applicable, in accordance with the Agreement.

**4. OBLIGATIONS OF PALANTIR**

With regard to its use and/or disclosure of PHI:

4.1 Safeguards. Palantir shall implement and use reasonable and appropriate administrative, physical, and technical safeguards, and comply with the applicable requirements of the Security Rule with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this BAA.

4.2 Reporting.

4.2.1 Palantir shall report to Customer, within a reasonable time frame , any successful Security Incident of which Palantir becomes aware. Notice is hereby deemed provided, and no further notice will be provided, for (a) unsuccessful Security Incidents, including, but not limited to, routine occurrences of pings and other broadcast attacks on a firewall, denial of service attacks, port scans, or unsuccessful login attempts; or interception of encrypted information, media or devices where the key is not compromised, or any combination of the above.

4.2.2 Palantir shall, following discovery of a Breach of Unsecured PHI or use or disclosure of PHI in a manner not permitted by the Agreement and/or applicable law, notify Customer of such Breach, use or disclosure as required at 45 C.F.R. § 164.410, without unreasonable delay, and in no event more than five (5) business days after Palantir's discovery of the Breach, use or disclosure, unless Palantir is prevented from doing so by 45 C.F.R. § 164.412 concerning law enforcement investigations. Palantir's obligation to report or notify under this BAA, including under 4.2.1 and 4.2.2, is not and will not be construed as an acknowledgement by Palantir of any fault or liability with respect to any claims arising from this BAA.

4.3 Mitigation. Palantir shall mitigate to the extent practicable any harmful effect from any use or disclosure of PHI in violation of this BAA or applicable law.

4.4 Subcontractors. Palantir shall, in accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure pursuant to a duly executed BAA that any Subcontractor that uses, discloses, accesses, creates, receives, maintains or transmits PHI on behalf of Palantir, agrees to restrictions and conditions that

apply to Palantir under this BAA with respect to that PHI that are at least as stringent as those set forth herein.

4.5 Access and Amendment. If Palantir maintains PHI in a Designated Record Set on behalf of Customer, Palantir shall provide Customer access to such PHI for inspection, copying, and amendment of PHI by Customer as necessary under 45 C.F.R. § 164.524 and 45 C.F.R. § 164.526. Customer acknowledges and agrees that Customer is solely responsible for the form and content of PHI maintained by Customer within the Palantir Technology and related services, including whether Customer maintains such PHI in a Designated Record Set within the Palantir Technology. Palantir will provide Customer with access to Customer's PHI via the Palantir Technology so that Customer may fulfill its, or a Covered Entity's, obligations, as applicable, under HIPAA with respect to Individuals' rights of access and amendment, but will have no other obligations to Customer or any Individual with respect to the rights afforded to Individuals by HIPAA with respect to rights of access or amendment of PHI. Customer is responsible for managing its use of the Palantir Technology to appropriately respond to such Individual requests.

4.6 Accounting of Disclosures. Palantir shall maintain and make available to Customer the information about Disclosures of PHI made by Palantir that is required for Customer to respond to an Individual's request for an accounting of Disclosures as necessary under 45 C.F.R. § 164.528.

4.7 Government Access to Records. Palantir shall make its internal practices, books and records relating to the use or disclosure of PHI under this BAA available to the U.S. Secretary of HHS for purposes of determining Customer's or a Covered Entity's compliance with the Privacy Rule. Nothing in this section shall waive any applicable privilege or protection, including with respect to Confidential Information.

**5. OBLIGATIONS OF CUSTOMER**

5.1 Safeguards. Customer shall obtain any and all necessary authorizations, consents, and other permissions that may be required under the Confidentiality Requirements and/or other applicable law or regulation prior to providing Palantir any PHI under this BAA. Customer is responsible for implementing and using appropriate administrative, physical, and technical safeguards at all times to ensure the confidentiality, privacy, security, and integrity of its PHI in compliance with the Confidentiality Requirements, including in the configuration of systems, applications, and software Customer controls and uses in connection with the Palantir Technology and Professional Services. Customer shallnot request or cause Palantir to make a use or disclosure of PHI in a manner that does not comply with the Confidentiality Requirements or this BAA.

5.2 No PHI Outside Service. Customer will not include PHI in information Customer submits to Palantir's personnel through a technical support request or other channels outside of the Service or Palantir-designated data ingestion process and represents, warrants and covenants that any information submitted through such a request or other channel outside of the Service is not PHI.

5.3 Restrictions on Use or Disclosure. In the event that Customer honors a request to restrict the use or

disclosure of PHI pursuant to 45 C.F.R. § 164.522(a) or a Covered Entity makes revisions to its notice of privacy practices that place additional limitations on uses or disclosures of PHI or agrees to a request by an Individual for confidential communications under 45 C.F.R. § 164.522(b), Customer agrees not to provide Palantir with any PHI that is subject to any of those restrictions or limitations to the extent such may limit Palantir's ability to use and/or disclose PHI as permitted or required under this BAA unless Customer notifies Palantir in writing of the restriction or limitation and Palantir agrees in writing to honor the restriction or limitation.

**6. TERM AND TERMINATION OF BAA**

6.1 Term. The Term of this BAA shall be effective as of the Effective Date and shall terminate on the latter of

(a) the date that the Agreement is terminated or expires, or (b) the date on which PHI is permanently deleted from the Palantir Technology; provided, however, that termination shall not affect the respective obligations or rights of the Parties arising under this BAA prior to the effective date of termination, all of which shall continue in accordance with their terms.

6.2 Obligations Upon Termination. Upon termination of this BAA for any reason, Palantir shall return or destroy (at Palantir's option) all PHI received from Customer in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Agreement. If PHI is destroyed, Palantir agrees to provide Customer with confirmation of such destruction upon request. In the case of PHI for which it is not feasible to return or destroy, Palantir 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 destruction infeasible and/or as otherwise Required by Law, for so long as Palantir maintains such PHI.

**7. LIABILITY**

7.1 The total combined liability of either Party and its Affiliates towards the other Party and its Affiliates under or in connection with this BAA will be the liability cap, and subject to the liability limitations, set forth in the Agreement for the relevant Party.