Splunk Business Associate Agreement

This Business Associate Agreement is incorporated into and forms part of the Splunk General Terms and applicable Order, or such other written or electronic agreement between Splunk and Customer for the purchase of Splunk HIPAA-certified Hosted Services ("**Agreement**").

THIS BUSINESS ASSOCIATE AGREEMENT ("**BAA**") is made as of the Effective Date (defined below)

BETWEEN

(1) _____, a company incorporated in _____ with a principal place of business at _____, together with any Affiliates, as defined in the Agreement, which are authorized to use the Splunk Offerings under the Agreement (and provided an Affiliate is not subject to a separate Agreement with Splunk), collectively referred to as "**Customer**"; and

(2) **Splunk Inc.**, whose principal place of business is at 270 Brannan St., San Francisco, CA 94107 ("**Splunk**").

Each a "**Party**" and together, the "**Parties**."

Instructions

This BAA has been pre-signed on behalf of Splunk.

To execute this BAA, Customer must:

(a) complete the information in the section above;

(b) verify that the information is accurate, complete and is the same as the information about Customer provided in the Agreement; and

(c) submit the validly completed, signed and unmodified BAA to Splunk by email at: dpacontracts@splunk.com or execute the BAA online.

This BAA will become effective as of the date that the HIPAA-certified Hosted Services start as listed in the applicable Order ("**Effective Date**"). This BAA will be deemed legally binding upon receipt by Splunk of a fully executed copy pursuant to the instructions above and supersedes any prior agreements between Customer and Splunk concerning the processing of Protected Health Information.

How This BAA Applies

In the event of any conflict or inconsistency between the terms of the Agreement and this BAA, the latter shall prevail, but only to the extent of the conflict or inconsistency. Any terms which are not defined in the Agreement are as defined below in this BAA.

Splunk BAAs are not available for and do not apply to: Trials, Evaluations, Beta or Free Licenses. A BAA executed in connection with any such licenses will be deemed null and void. This BAA applies only to paid subscriptions to the HIPAA-certified Hosted Services and does not apply to on-premise component(s) of a hybrid Offering or to Hosted Services that are not HIPAA-certified.

During the term of the Agreement, Customer may be acting as a: 1) Covered Entity; 2) Business Associate of a Covered Entity; 3) or a Business Associate of a Business Associate ("Secondary BA"). Splunk may have access to Protected Health Information processed through the HIPAA-certified Hosted Services and may be acting as a Business Associate under HIPAA Rules.

This BAA sets forth Splunk's obligations as a Business Associate only and does not require Splunk to carry out Customer's obligations as a Covered Entity, Business Associate, or Secondary BA.

Agreement

Subject to the terms of the Agreement, the below terms and conditions apply to Splunk as a Business Associate. The Parties acknowledge and agree that Splunk does not maintain Protected Health Information in a Designated Record Set.

1. Obligations and Activities of Splunk

Splunk agrees to:

(a) Not Use or Disclose Protected Health Information other than as permitted or required by this BAA or as Required By Law. Splunk will not disclose, capture, maintain, scan, index, transmit, share, or Use Protected Health Information for any activity not authorized under the Agreement or this BAA;

(b) Comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information to prevent its Use or Disclosure except as provided for by the Agreement and this BAA or as Required by Law, by maintaining a reasonable and appropriate privacy and security program that includes administrative, technical, and physical safeguards that Splunk takes to protect the confidentiality, integrity, and availability of Protected Health Information that it creates, receives, maintains, or transmits on behalf of Customer;

(c) Report to Customer the: (i) Use or Disclosure of Protected Health Information not permitted or required under this BAA of which Splunk becomes aware; (ii) Breaches of Unsecured Protected Health Information of which it becomes aware without unreasonable delay as required by 45 CFR 164.410; and (iii) Security Incident(s) of which it becomes aware, subject to section 1(d) below. The timing of other reporting will be made consistent with Splunk's and Customer's legal obligations. Splunk's obligation to report under this section is not and will not be construed as an acknowledgement of any fault or liability with respect to any Use, Disclosure, Breach, or Security Incident. Splunk's notice of Breaches of Unsecured Protected Health Information shall include, to the extent possible, the information specified in 45 CFR 164.410;

(d) Splunk monitors routine and ongoing unsuccessful attempts to gain unauthorized Access to Splunk's Information System, including but not limited to pings, port scans, denial of service attacks, unsuccessful log-on attempts, and other broadcast attacks on Splunk's firewall. Notwithstanding section 1(c)(iii) above, Customer acknowledges and agrees that even if such events constitute a Security Incident, Splunk will not be required to provide any notice under this BAA provided that no such incident results in unauthorized Access, Use, or Disclosure of Electronic Protected Health Information;

(e) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), require any Subcontractors that may create, receive, maintain, or transmit Protected Health Information on behalf of Splunk to agree in writing to: (i) the same or more stringent restrictions and conditions that apply to Splunk with respect to such Protected Health Information; (ii) appropriately safeguard the Protected Health Information; and (iii) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule;

(f) Provide Customer with reasonable assistance, including through the functionality of the HIPAA-certified Hosted Services, in fulfilling its obligations regarding Individual access and amendment pursuant to 45 CFR 164.524 and 45 CFR 164.526. Splunk reserves the right to charge for assistance rendered at Customer's request through means other than service functionality;

(g) Within thirty (30) days of receipt of a written request from Customer, Splunk will provide Customer with information reasonably required for Customer to respond to an Individual request for an accounting of Disclosures pursuant to 45 CFR 164.528;

(h) Make its internal practices, books, and records relating to the Use and/or Disclosure of Protected Health Information received from the Customer available to the Secretary of the Department of Health and Human Services for purposes of determining Customer's compliance with the HIPAA Rules, subject to attorney-client and other applicable legal privileges or protections;

(i) Make reasonable efforts to Use, Disclose, and request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request;

(j) Upon request, provide Customer with proof of Splunk's annual audit evidencing compliance with the Security Rule and Breach Notification requirements for the processing of Protected Health Information; and

(k) Take reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to Splunk of a Use or Disclosure of Protected Health Information by Splunk or its Subcontractors in violation of the requirements of this BAA.

2. Obligations and Responsibilities of Customer

(a) Customer will comply fully with its obligations under the HIPAA Rules.

(b) Customer will not place any restrictions in a notice of privacy practices under 45 CFR 164.520 that will conflict with applicable law or Splunk's obligations under this BAA. Customer hereby agrees that any reports, notification, or other notice by Splunk will be provided as set forth in the Agreement. Customer agrees that any reports, notifications, or other notice by Splunk pursuant to this BAA may be made electronically.

(c) Customer will notify Splunk of any changes in, or revocation of, the permission by an Individual to Use or Disclose Protected Health Information, to the extent that such changes may affect Splunk's Use or Disclosure of Protected Health Information.

(d) Customer will notify Splunk of any restriction on the Use or Disclosure of Protected Health Information that Customer has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Splunk's Use or Disclosure of Protected Health Information.

(e) Customer will be responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with its obligations under HIPAA. Without limitation, it is Customer's responsibility to implement privacy and security safeguards in the systems, applications, and software the Customer controls, configures, or otherwise makes accessible in accordance with the Documentation. For avoidance of doubt, this provision does not conflict with or override any of Splunk's privacy or security obligations as set forth in the Agreement or this BAA.

(f) Customer will not ask Splunk to Use or Disclose Protected Health Information in any manner that would be impermissible under Subpart E of 45 CFR Part 164 if done by Customer (or Customer's Covered Entity, if applicable). Nothing herein will restrict Splunk from using Protected Health Information for Data Aggregation or management, administration, and legal responsibilities of Splunk as permitted by this BAA.

(g) Customer will not transmit or include Protected Health Information in information Customer submits to Splunk support or professional services personnel, including within the subject or body of a diagnostic file submitted in the course of filing a support ticket.

3. Permitted Uses and Disclosures by Splunk

(a) Splunk may only Use or Disclose Protected Health Information as necessary to perform HIPAA-certified Hosted Services as described in the Agreement.

(b) Splunk may not Use or Disclose Protected Health Information in a manner that would violate the privacy of an Individual's identifiable health information as outlined in Subpart E of 45 CFR Part 164 if done by Customer (or by Customer's Covered Entity, if applicable), except for the specific Uses and Disclosures set forth below in this section 3.

(c) Except as authorized under the HIPAA Rules, Splunk may not directly or indirectly receive renumeration from or on behalf of a recipient of Protected Health Information in exchange for the Protected Health Information. Splunk will not engage in any communication using Protected Health Information contained within Customer Content which may be deemed "marketing" under the HIPAA Rules.

(d) Splunk may Use and Disclose Protected Health Information for the proper management and administration of Splunk's business and to carry out its legal responsibilities provided that: (i) the Disclosure is Required by Law; or (ii) Splunk obtains reasonable assurance from the person to whom the Protected Health Information is

Disclosed that it will be held confidentially and Used or further Disclosed only as Required By Law or for the purposes for which it was Disclosed to the person; and (iii) the person notifies Splunk of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

(e) Splunk may provide Data Aggregation services to Customer relating to the Health Care Operations of Customer or if Customer is a Business Associate then to Customer's Covered Entity only to the extent that Customer's use of the HIPAA-certified Hosted Services may be deemed Health Care Operations.

(f) In providing the HIPAA-certified Hosted Services, Splunk may incidentally collect fragments of Protected Health Information in metadata generated by use of the Hosted Services. Such Protected Health Information does not include Customer Content. Splunk may de-identify any such Protected Health Information in accordance with 45 CFR 164.502(d) of the HIPAA Rules and use, modify and Disclose such de-identified data as permitted by law.

4. Term and Termination

(a) **Term**. This BAA is effective as of the Effective Date and will terminate upon the earlier of (i) termination or expiration of the Agreement or (ii) termination of this BAA under section 4(b) or 4(c) below.

(b) **Termination for Cause by Customer**. Notwithstanding any provision in the Agreement to the contrary, a material breach by Splunk of any provision of this BAA will constitute a material breach of this BAA and applicable sections of the Agreement. Upon Customer's knowledge of a breach or violation of this BAA by Splunk, Customer may require Splunk to cure the breach or end the violation. If Splunk does not cure the breach or end the violation, or if no cure or end of violation is possible, Customer may either (i) immediately terminate this BAA (and applicable sections of the Agreement) upon written notice to Splunk or (ii) if termination is not feasible, Customer will report the violation to the Secretary.

(c) **Termination for Cause by Splunk**. Upon Splunk's knowledge of a pattern of activity or practice of Customer that constitutes a material breach or violation of Customer's obligations under this BAA or the Agreement, Customer must take reasonable steps to cure the breach or end the violation. If Customer does not cure the breach or end the violation, Splunk may either (i) immediately terminate this BAA (and applicable sections of the Agreement) upon written notice to Customer or (ii) if termination is not feasible, Customer will report the violation to the Secretary.

(d) **Obligations Upon Termination**.

(i) Except as provided in subsections (ii) and (iii) below, upon termination of this BAA for any reason, Splunk will return or irretrievably destroy all Protected Health Information, in any form, received from Customer or created, maintained, or received by Splunk on behalf of Customer, or in possession of Subcontractors or agents of Splunk, including copies thereof, if it is feasible to do so.

(ii) In the event the Parties determine that returning or destroying the Protected Health Information is not feasible, Splunk will continue to limit its Uses and Disclosures of Protected Health Information under the terms of this BAA for so long as such Protected Health Information remains under Splunk's possession or control.

(iii) For the avoidance of doubt, Splunk's obligations to return and/or destroy the Protected Health Information as set forth in section 4(d)(i) will not apply to any Protected Health Information which has been de-identified in accordance with section 3(f) of this BAA. Customer acknowledges and agrees that Splunk shall be free to continue to use de-identified data without restriction after the termination or expiration of this BAA.

5. Miscellaneous

(a) **HITECH Act Compliance**. The Parties acknowledge that the HITECH Act includes changes to the Privacy Rule and the Security Rule that affect the requirements for Business Associates and Business Associate Agreements. Each Party agrees to comply with the applicable provisions of the HITECH Act and any applicable regulations that the Department of Health and Human Services issues in connection with the HITECH Act.

(b) **Regulatory References**. A reference in this BAA to a section in the HIPAA Rules means the section in effect or as amended.

(c) **Amendment**. The Parties agree to amend this BAA from time to time as is reasonably necessary for Customer to comply with the requirements of the HIPAA Rules.

(d) **No Third-Party Beneficiaries**. Except as expressly provided for in the Privacy Rule, there are no third-party beneficiaries to this BAA. Splunk's obligations are to Customer only.

(e) **All other terms of the Agreement** apply to this BAA, including without limitation, choice of law, venue and limitation of liability.

(f) **Counterparts**. This BAA may be executed in two or more counterparts, each of which may be deemed an original.

Definitions

(a) **HIPAA Rules**. "HIPAA Rules" will mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Part 160 and Part 164, including as amended by the HITECH Act (defined below).

(b) **HITECH Act**. The "HITECH Act" will mean Subtitle D of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009.

(c) **Terms Defined in the HIPAA Rules**. The following terms used in this BAA will have the same meaning as those terms in the HIPAA Rules: Access, Breach, Business Associate, Covered Entity, Data Aggregation, Designated Record Set, Disclosure, Disclose, Health Care Operations, Electronic Protected Health Information, Individual, Information System, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Security Rule, Subcontractor, Unsecured Protected Health Information, and Use.

IN WITNESS WHEREOF, the Parties have executed this BAA as of the date of the last signature below ("Effective Date").

CUSTOMER		**SPLUNK INC.**	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____