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.

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 incidental 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.

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;

(b) Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164, as applicable and feasible, with respect to Electronic Protected Health Information to prevent its Use or Disclosure except as provided for by this BAA;

(c) Report to Customer the: i) Use or Disclosure of Protected Health Information not provided for by this BAA; ii) Breaches of Unsecured Protected Health Information of which it becomes aware without unreasonable delay, and in no case later than sixty (60) calendar days after discovery, as required by 45 CFR 164.410; and iii) Security Incident(s). 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. The Breach notification required by this section shall include, to the extent possible: (a) a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known; (b) a description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); and (c) a brief description of what the Covered Entity involved is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches;

(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), if applicable, require any Subcontractors that create, receive, maintain or transmit Protected Health Information on behalf of Splunk to agree in writing to (1) the same restrictions and conditions that apply to Splunk with respect to such Protected Health Information, (2) appropriately safeguard the Protected Health Information and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule;

(f) Provide Customer with reasonable assistance, 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 such assistance;

(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; and

(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 compliance with the HIPAA Rules, subject to attorney-client and other applicable legal privileges or protections.

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 agrees that any reports, notifications or other notice by Splunk pursuant to this BAA may be made electronically. Customer will provide Splunk with the designated contact information for reporting purposes (e.g., name, email address, etc.) and will update it as needed during the term of this BAA.

(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 connection with the Agreement and uploads to Splunk.

(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.

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 Sections 3 (c), (d) and (e).

(c) Splunk may Use and Disclose Protected Health Information to carry out its legal responsibilities under the Agreement and this BAA 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.

(d) 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, to the extent that HIPAA-certified Hosted Services may be deemed Health Care Operations.

(e) In providing the Hosted Services, Splunk may collect incidental Protected Health Information contained in metadata generated by use of the Hosted Services. Such incidental Protected Health Information does not include Customer Content. Splunk may de-identify any such incidental Protected Health Information in

accordance with section 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 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 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, if it is feasible to do so. For clarity, Splunk will retain no copies of the Protected Health Information except in circumstances described in sections (ii) and (iii) below.

(ii) In the event the Parties determine that returning or destroying the Protected Health Information is neither practical nor feasible, Splunk will continue to limit its Uses and Disclosures under the terms of this BAA for so long as it remains under Splunk 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(c)(i) will not apply to any Protected Health Information which has been de-identified in accordance with Section 3(e) 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.

(e) **Survival**. Sections 4(d) and 5 of this BAA will survive any termination of this BAA.

5. Miscellaneous

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

(b) **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.

(c) **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.

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

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

Definitions

(a) **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, Person, Protected Health Information, Required By Law, Secretary, Security Incident, Security Rule, Subcontractor, Unsecured Protected Health Information and Use.

(b) **Affiliate**. "Affiliate" is as defined in the Agreement.

(c) **Customer Content**. "Customer Content" is as defined in the Agreement.

(d) **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).

(e) **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.

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:	DocuSigned by: Jaime Hildebrand F52A29DF2C46470...
Name:	_____	Name:	Jaime Hildebrand
Title:	_____	Date:	_____
Date:	_____		