Talend, Inc. Business Associate Agreement

(Last Updated March 2021)

This **BUSINESS ASSOCIATE AGREEMENT** ("**BAA**") is entered into as of the **Effective Date** (as defined in the Agreement), by Talend and the party entering into the Agreement with Talend that refers to this BAA (the "**Customer**"). This BAA shall be deemed a part of the Agreement between Talend and Customer governing the contractual relationship between Talend and Customer. The Agreement may involve access to Protected Health Information (as defined below) from Customer. This Addendum defines Talend and Customer respective rights and responsibilities with respect to the privacy and security of certain health information in connection with certain federal laws. In the event of a conflict between the terms and conditions of this BAA and the Agreement, the terms and conditions of this BAA shall supersede and take precedence. All capitalized terms used in this Addendum and not defined in Section 1 of this Addendum shall have the meanings given to them in the Agreement.

Whereas, in order to execute this BAA, Customer must

1. Complete the information in the signature box and sign the BAA on page 6;

2. Send the completed and signed BAA to Talend by email, indicating the Customer's name to legal@talend.com.

Whereas, Customer and Talend (the "**Parties**") now wish to enter into the BAA as further described below.

Now Therefore, in furtherance of the foregoing and upon due consideration resulting from the Parties' compliance with HIPAA and HITCH (as defined below), the adequacy and receipt of which is hereby acknowledged, the parties agree as follows as of the Effective Date:

1. *Definitions:*

For purposes of this BAA, each of the following capitalized terms shall have the meaning set forth in this Section. All other capitalized terms in this BAA shall have the meaning given to them in the Agreement. Except as the context of a provision dictates otherwise, a term used in this BAA and not defined in this Section or in the Agreement shall have the meaning given to it under HIPAA or HITECH, as applicable.

(a) "**Breach**" shall have the same meaning as the term "breach" in 45 CFR § 164.402 but limited in application to Unsecured Protected Health Information.

(b) "**Business Associate**" shall have the same meaning as the term "business associate" in 45 CFR § 160.103, and in reference to the party to this BAA, shall mean Talend.

(c) "**CFR**" shall mean the Code of Federal Regulations.

(d) "**Covered Entity**" shall have the same meaning as the term "covered entity" in 45 CFR § 160.103, and in reference to the party to this BAA, shall mean Customer.

(e) "**Designated Record Set**" shall have the same meaning as the term "designated record set" in 45 CFR § 164.501.

(f) "**HIPAA**" shall mean the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder relating to the privacy and security of Protected Health Information and breach notification, as such statute and regulations may be amended from time to time.

(g) "**HITECH**" shall mean the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and the regulations promulgated thereunder relating to the privacy and security of protected health information, as such statute and regulations may be amended from time to time.

(h) "**Individual**" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

(i) "**Privacy Rule**" shall mean the standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

(j) "**Protected Health Information/Electronic Protected Health Information**" shall have the same meaning as the terms "protected health information" and "electronic protected health information," respectively, in 45 CFR § 160.103, limited to the information created, received, maintained, or transmitted by a Business Associate from or on behalf of a Covered Entity.

(k) "**Required by Law**" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

(l) "**Secretary**" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

(m) "**Security Rule**" shall mean the standards for Security of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and C.

(n) "**Subcontractor**" shall mean a person, not acting as a member of the Business Associate's workforce, to whom Business Associate delegates a function, activity, or service: (i) that is subject to the requirements of this BAA; and (ii) for which the person creates, receives, maintains, or transmits Protected Health Information.

(o) "**Unsecured Protected Health Information**" shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402, but limited to Protected Health Information.

2. *Obligations and Activities of Business Associate:*

2.1. Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this BAA or as Required by Law.

2.2. Business Associate agrees to use appropriate physical, technical, and administrative safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this BAA. These safeguards shall include, but not be limited to, policies and procedures for reasonably and appropriately protecting the confidentiality, integrity and availability of Electronic Protected Health Information. With respect to such information, Business Associate shall meet the requirements of the Security Rule that apply to business associates.

2.3. Business Associate agrees to report in writing to Covered Entity any use or disclosure of Protected Health Information not provided for by this BAA and any Security Incidents within the meaning of 45 CFR § 164.304, of which it becomes aware. Notice is deemed provided, and no further notice will be given, with respect to routine unsuccessful attempts at unauthorized access to ePHI such as pings and other broadcast attacks on firewalls, denial of service attacks, failed login attempts, and port scans. Business Associate shall provide a summary of such unsuccessful Security Incidents, at an aggregate level, upon request of Covered Entity once a year. In the event of a Breach of Unsecured Protected Health Information by Business Associate, Business Associate shall notify Covered Entity of the Breach in accordance with the requirements under 45 CFR § 164.410. Incidents under this section shall be reported without unreasonable delay and in no case later than thirty (30) calendar days after discovery of the incident, unless a law enforcement delay applies pursuant to 45 CFR § 164.412. In the event of a law enforcement delay, Business Associate shall notify Covered Entity within the time frame required by such section.

2.4. Business Associate shall, through written agreement, require any Subcontractor to agree to restrictions and conditions at least as strict as those that apply through this BAA to Business Associate with respect to Protected Health Information. Business Associate may disclose all or some of the terms of this BAA to any of its Subcontractors to secure its compliance with such restrictions and conditions.

2.5. To the extent Business Associate maintains in its systems Covered Entity's Protected Health Information, and at Covered Entity's reasonable and timely request, pursuant to a request by an Individual, Business Associate shall provide Covered Entity with Protected Health Information that Business Associate maintains in a Designated Record Set within fifteen calendar days of receipt of notice of an Individual's request to allow Covered Entity to comply with the requirements under 45 CFR § 164.524.

2.6. To the extent Business Associate maintains in its systems Covered Entity's Protected Health Information, and at Covered Entity's reasonable and timely request, pursuant to a request by an Individual, Business Associate shall make Protected Health Information that it maintains in a Designated Record Set available to Covered Entity for amendment within fifteen calendar days of receipt of notice of an Individual's request to allow Covered Entity to comply with the requirements under 45 CFR § 164.526.

2.7. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary in a time and manner designated by the Secretary, for purposes of the Secretary's determining Covered Entity's compliance with the Privacy Rule.

2.8. Business Associate agrees to document disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with the requirements under 45 CFR § 164.528. Upon Covered Entity's reasonable and timely request, Business Associate shall provide Covered Entity with such accounting within fifteen calendar days of receipt of notice of an Individual's request to allow Covered Entity to comply with the requirements under 45 CFR § 164.528.

2.9. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s). Notwithstanding the foregoing, the Parties do not intend for Covered Entity to delegate any HIPAA regulated functions or obligations to Business Associate.

2.10. Business associate may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity except for the specific uses and disclosures set forth below in Sections 3(c) and (d).

3. *Permitted Uses and Disclosures by Business Associate:*

Except as otherwise limited in this BAA, Business Associate may use or disclose Protected Health Information to:

(a) Perform obligations, functions, and activities as necessary to perform the services set forth by the Parties in the Agreement;

(b) Perform its obligations under this BAA;

(c) Conduct activities for its own proper management and administration or carry out its own legal responsibilities, provided that any disclosure of Protected Health Information for such purpose shall be either: (i) Required By Law; or (ii) made after Business Associate obtains reasonable assurances from the recipient of the Protected Health Information that the Protected Health Information will be held confidentially, that it will be used and disclosed further only for the purpose for which it was disclosed to the recipient, and that the recipient will notify Business Associate of any instances of which it becomes aware that the confidentiality of the Protected Health Information has been breached;

(d) Provide data aggregation services relating to the health care operations of Covered Entity; and

(e) Report violations of law in accordance with 45 CFR § 164.502(j)(1).

4. *De-Identified Data:*

Business Associate may use Protected Health Information to de-identify the information in accordance with 45 CFR § 164.514(a)-(c). De-identified information is not considered Protected Health Information and Business Associate may further use and disclose such information for its own business purposes.

5. *Obligations of Covered Entity:*

5.1. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions.

(a) Covered Entity shall notify Business Associate of any provisions in its notice of privacy practices prepared in accordance with 45 CFR § 164.520 that may affect Business Associate's responsibilities with respect to Protected Health Information and of any modifications thereto.

(b) Covered Entity shall notify Business Associate of: (i) any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information; and (ii) any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

5.2. Permissible Disclosures by Covered Entity. Covered Entity shall make a reasonable effort not to provide Business Associate more than the minimum Protected Health Information necessary for Business Associate to perform functions that are permitted or required under this BAA and shall implement and apply other physical, technical and administrative safeguards to transmit Protected Health Information to Business Associate in a manner that meets the requirements of HIPAA and HITECH, as applicable.

5.3. Necessary Consents. Covered Entity shall obtain or have obtained all necessary authorizations, consents, and other permissions that may be required under applicable law to provide or arrange for the provision of Protected Health Information to Business Associate.

5.4. Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under HIPAA or HITECH if done by Covered Entity except as specified in Sections 3(c) and (d).

5.5. Specified Compliance Measures. Covered Entity agrees to comply with the configuration, transmission, and other requirements set forth in the "Operating Talend products in Compliance with HIPAA" (the, "**Document**"), as amended from time to time, the current version of which is attached hereto as Exhibit A and incorporated and made part of this BAA. Business Associate agrees to notify Covered Entity as soon as practicable of any amendment to the Document that is more restrictive with regard to Covered Entity than the terms of the Document prior to such amendment.

6. *Term and Termination*

6.1. The term of this BAA shall begin as of the Effective Date and shall terminate as provided elsewhere in this BAA or when all of the Protected Health Information is destroyed or returned to Covered Entity or its designee.

6.2. If Covered Entity knows of a pattern of activity or practice by Business Associate that constitutes a material breach or violation of Business Associate's obligations under the BAA, Covered Entity shall notify Business Associate of the breach and of the reasonable period during which Business Associate may take measures to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within that period, Covered Entity shall terminate this BAA and, the extent applicable, its Agreement with Business Associate for the provision of services pertaining to Protected Health Information as soon as feasible.

6.3. Upon termination of this BAA, Business Associate shall have the following obligations:

(a) Except as provided in paragraph (b) of this section, Business Associate shall return or, at Covered Entity's direction, destroy all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business associate shall retain no copies of Protected Health Information.

(b) In the event that Business Associate determines that returning or destroying any Protected Health Information is infeasible, Business Associate shall:

(i) Retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(ii) Return to Covered Entity or destroy the remaining Protected Health Information that Business Associate still maintains in any form;

(iii) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information to prevent use or disclosure of the information, other than as provided for in this section, for as long as Business Associate retains the Electronic Protected Health Information;

(iv) Not use or disclose Protected Health Information retained by Business Associate other than for the purposes for which such information was retained and subject to the same conditions set out at Sections 2 and 3 above which applied prior to termination; and

(v) Return to Covered Entity or destroy the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

7. *Miscellaneous:*

7.1. Regulatory References. A reference in this BAA to a section in HIPAA or HITECH, as applicable, means the section as in effect, as amended.

7.2. Amendment. Covered Entity and Business Associate agree to take appropriate action to amend this BAA from time to time as necessary for the Parties to comply with the requirements of HIPAA or HITECH, as each may be amended or construed by courts of applicable jurisdiction or the Secretary from time to time. Each such amendment shall be made by and, unless the Parties mutually agree, effective as of the applicable compliance date for the change in rules or interpretation. The Parties may amend or terminate this BAA in a writing executed by authorized representatives of each Party.

7.3. Communications. Written communications from one Party to the other shall be provided as set forth in the Agreement except as the receiving Party specifies to the other Party in writing.

7.4. Relationship. With respect to all functions that Business Associate performs on behalf of Covered Entity that involve Protected Health Information, the Parties shall have no relationship other than that of independent contractors.

7.5. Disclosure of Terms of Agreement. Business Associate may disclose some or all of the terms of this BAA to a Subcontractor or potential Subcontractor.

7.6. Survival. The respective rights and obligations of Business Associate under Sections 6.3 of this BAA shall survive the termination of this BAA and the Agreement.

7.7. Interpretation. Any ambiguity in this BAA and the Agreement shall be resolved to permit Covered Entity and Business Associate to comply with their respective obligations under HIPAA and HITECH. The Parties understand that Business Associate shall rarely, if ever, access Protected Health Information and shall perform its obligations under this BAA in a manner that is consistent with that understanding. In the event of any conflict between the provisions of this BAA and other provisions of the Agreement with regard to Protected Health Information, the provisions of this BAA shall govern.

7.8 Integration. This BAA constitutes the complete agreement between Covered Entity and Business Associate relating to the matters specified in this BAA and supersedes all prior representations or agreements, whether oral or written, with respect to such matters.

This BAA has been signed on behalf of each of the Parties by a duly authorized signatory.

FOR AND ON BEHALF OF TALEND, INC.:	**FOR AND ON BEHALF OF CUSTOMER:**
Signature: DocuSigned by: Aaron Ross A0739E3Z1ED84A4...	**Signature:**
Name: Aaron Ross	**Name:**
Title: General Counsel	**Title:**
Date: 08-Mar-2021	**Date:**

Effective Date: 08-Mar-2021 **(if blank, then the Effective Date is the last indicated date of execution)**

Exhibit A

1. Operating Talend Cloud Services in Compliance with HIPAA

Summary:

Talend Cloud utilizes cloud services providers to process customer data, including Amazon Web Services (AWS) and Microsoft Azure infrastructures . Talend has entered into a Business Associate Agreement (BAA) with these cloud services providers to ensure that Talend services are offered in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Talend customers who wish to have Electronic Protected Health Information (ePHI) processed by Talend in compliance with HIPAA, and to leverage these agreements, must agree to comply with the following rules.

This document supplements, and must be read jointly with the Talend Cloud Security Architecture Overview.

For a complete list of customer responsibilities, please refer to the HIPAA Controls Checklist - Talend & Customer Responsibility Share.xlsx.

Talend Cloud HIPAA Security Requirements:

1. Customer must ensure that ePHI is not present in metadata

   This includes:

   - User, account, and job names
   - For database sources and targets: user, database, schema, table, and column names
   - For web service sources: dataset and field names

2. Customer must ensure not to transmit ePHI to Talend in support request or grant access to ePHI during professional services engagement

   The customer must ensure that ePHI is not transmitted to Talend through any medium (including in-app messaging, support requests, and email).

   If a customer needs to send ePHI to Talend as part of a support request or grant access to ePHI to Talend during professional services engagement, the customer should work with Talend Support and Professional Services Teams, without sending ePHI, to establish a secure data transmission mechanism when needed.

   In the event that a customer needs access to logging information that is not available through the product activity logs, the customer may open a support case with Talend.

3. Customer remains responsible for HIPAA-compliance and configuration of their data sources and destinations

   Talend shall be responsible for the protection and compliance of customer data strictly while it is being stored, processed or transmitted within Talend software and services.

   It is acceptable to transmit both PHI and non-PHI data within the same Talend account, as long as the account is configured to prevent unauthorized access, deletion or modification of the PHI data.

   Configuration of the customer source and destination databases, applications, data warehouses and/or filesystems are the customer's responsibility. Talend only transmits data to the location and service the customer specifies. The customer shall ensure that the data destination is a secured environment, configured in accordance with HIPAA requirements and compliant with industry-standard best practices. Talend shall not be liable for any noncompliance associated with customer source or destination repositories.

4. Customer's credentials to access Talend software and services must be consistent with industry best practices

   Passwords must be complex and not easily guessed. Passwords should be unique to the Talend service and provisioned only on a need-to-know basis. Acceptable strong passwords will have the following characteristics:

   1) Must use characters from at least 3 of the following groups:

   - Uppercase characters (A-Z)
   - Lowercase characters (a-z)
   - Base 10 digits (0-9)
   - Non-Alphanumeric symbols (!, #, @, %, &, *)

2) Contains at least eight alphanumeric characters.

Talend recommends that customers not provision shared user accounts. In the event that a customer chooses to provision shared accounts, it will be the customer's responsibility to determine user identity in the event of an incident.

5. Customer shall ensure that any user for whom the customer has provisioned access have a valid need-to-know, and has received proper HIPAA security awareness training.

   Customers shall ensure that user access rights are terminated when no longer needed. The customer must report to Talend any known or suspected breaches of a customer account as well as any known or observed, security weaknesses, incidents, account compromises or other abnormal or suspicious activity.

6. Customer shall ensure that it has backups of ePHI and is able to make ePHI available to end users as needed.

   While Talend maintains data backup, restore and disaster recovery processes, the Talend software and systems are not designed to function as final repositories for PHI.

2. Operating Stitch in Compliance with HIPAA

Stitch utilizes Amazon Web Services (AWS) infrastructure to process customer data, and Stitch has entered into a Business Associate Agreement (BAA) with AWS to ensure that Stitch services are offered in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Stitch customers who wish to leverage this agreement and have Electronic Protected Health Information (ePHI) processed by Stitch must agree to perform the following steps to ensure the data is protected in accordance with AWS and government requirements.

First, the customer must ensure that PHI is not present in metadata used by Stitch, including:

- User, account, and integration names
- For database sources: user, database, schema, table, and column names
- For web service sources: dataset and field names

The customer must also ensure that PHI is not transmitted in support requests to Stitch through any medium (including in-app messaging and email).

Second, the customer must only transmit PHI from the following HIPAA-compliant sources, configured as described:

- MySQL, MariaDB, Amazon Aurora MySQL Edition, Google Cloud SQL for MySQL, PostgreSQL, Amazon Aurora Postgres Edition, Google Cloud SQL for PostgreSQL, Microsoft SQL Server, Microsoft Azure SQL Database, MongoDB – either the SSH or SSL encryption options must be chosen to secure PHI, and the customer must ensure that their systems are appropriately patched and configured per industry-standard best practice to ensure a secure communication session.
- Salesforce.com – any configuration
- Zendesk – any configuration
- Desk.com – any configuration
- Amazon S3 CSV – any configuration
- SFTP – Configured paths, filenames and the first row of each file's data should strictly be metadata, not containing any PHI It is acceptable to transmit both PHI and non-PHI data within the same Stitch account, as long as the account is configured according to this document and PHI is only transmitted from the above sources.

Third, the customer must only transmit PHI to the following HIPAA-compliant destinations:

- Amazon Redshift
- Snowflake
- Google BigQuery
- Postgres – either the SSH or SSL encryption options must be used to secure

PHI, and the customer must ensure that their systems are appropriately patched and configured per industry standard best practice to ensure a secure communication session.

Configuration of the customer data warehouse is the customer's responsibility. Stitch only transmits data to the location and service the customer specifies. The customer shall ensure that this is a secured environment, configured in accordance with HIPAA requirements and compliant with industry-standard best practices. Stitch shall not be liable for any noncompliance associated with the data warehouse.

Fourth, customer-supplied credentials for Stitch to access their environment and to transmit data to the customer warehouse must be robust. Passwords must be complex and not easily guessed. Passwords should be unique to the Stitch service and shared only on a need-to-know basis.

Finally, the customer must activate the "Hide plain-text error messages in notification emails" setting in the Account Settings page of the Stitch web application. This ensures that PHI is not sent through email as part of an error message.