OKTA, INC.
HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement ("**BAA**") forms part of, and is subject to, the Okta Master Subscription Agreement (or other such titled written or electronic agreement addressing the same subject matter) between Okta and Customer governing Customer's use of the Service ("**Agreement**"). This BAA defines the rights and responsibilities of each party with respect to Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder, including but not limited to the HITECH Act and Omnibus Rule, as each may be amended from time to time (collectively, "**HIPAA**").

1. Defined Terms. For the purposes of this BAA, capitalized terms shall have the following meanings:

"**Business Associate**" shall generally have the same meaning as the term "business associate" defined in 45 CFR 160.103.

"**Covered Entity**" shall generally have the same meaning as the term "covered entity" defined in 45 CFR 160.103.

"**HIPAA Rules**" shall mean the Privacy, Security, Breach Notification and Enforcement Rules defined in 45 CFR 160 and 164.

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

"**HIPAA Service**" shall mean the products and services purchased by Customer under an Order Form that are designated by Okta as eligible to receive PHI as described in the Documentation, excluding Professional Services, Free Trial Service, and Non-Okta Products. Customer may use the HIPAA Service to store or transmit its PHI to the extent Okta meets, with respect to Customer, the definition of a Business Associate or Subcontractor.

"**Privacy Rule**" shall mean the Standards for Privacy of Individually Identifiable Health Information set forth in 45 CFR 160 and 164, Subparts A and E.

"**Protected Health Information**" or "**PHI**" shall have the same meaning as the term "protected health information" defined in 45 CFR 160.103, limited to the information electronically submitted to the HIPAA Service by or on behalf of Customer, in the course of performing the HIPAA Service under the Agreement.

"**Required By Law**" shall have the same meaning as the term "required by law" defined in 45 CFR 164.103.

"**Security Rule**" shall mean the Security Standards for the Protection of Electronic Protected Health Information defined in 45 CFR 160 and 164, Subparts A and C.

"**Subcontractor"** shall have the same meaning as the term "Subcontractor" defined in 45 CFR 160.103.

Capitalized terms used but not defined in this BAA will have the meaning assigned to them in the Agreement. The following terms used in this BAA shall have the same meanings as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Notice of Privacy Practices, Secretary, Security Incident, Unsecured Protected Health Information and Use.

2. Applicability. This BAA applies only to the Customer and those Customer Affiliates permitted under the Agreement that have purchased Okta's HIPAA Service.

3. Obligations of Okta.

3.1. Operational Obligations. Okta agrees to:

a) not use or disclose PHI other than as permitted in writing by Customer or required by this BAA or by law;

b) make reasonable efforts to limit uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure;

c) provide physical, technical, and administrative safeguards, consistent with the requirements of Subpart C of 45 CFR 164 (with respect to electronic PHI) as determined by Okta and as reflected in the Agreement. If Okta agrees as part of this BAA to carry out an obligation of Customer under the Privacy Rule, then Okta will comply with the requirements of the Privacy Rule applicable to such obligation;

d) obtain from any agent, including a Subcontractor to whom it provides PHI, reasonable assurances that it will adhere to restrictions and conditions that are at least as protective of the PHI provided by Customer as the restrictions and conditions that apply to Okta under this BAA with respect to such information;

e) report to Customer (i) Security Incidents (as defined in 45 CFR 164.304 and as further described below), (ii) the Breach of unsecured PHI (as defined in 45 CFR 164.402), or (iii) an access, acquisition, use or disclosure of PHI in violation of this BAA. The timing of reporting will be made consistent with Okta's and Customer's legal obligations. The Parties acknowledge and agree that this section constitutes notice by Okta to Customer of the ongoing existence and occurrence of attempted but unsuccessful Security Incidents (which shall include, but not be limited to, pings and other broadcast attacks on Okta's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access to, use, or disclosure of PHI) for which no additional notice to Customer shall be required. Okta'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, Security Incident or Breach. Customer acknowledges that details of PHI contained in the HIPAA Service (if any), stored in HIPAA Service logs will be subject to Okta's standard retention policy after which time such data will be deleted.

f) mitigate, to the extent reasonably practicable, any harmful effect that is known to Okta of a use or disclosure of PHI by Okta or its agents or subcontractors in violation of the requirements of this BAA; and

g) make internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Customer's compliance with the Privacy Rule; provided, however, that time incurred by Okta in complying with any such request that exceeds its legal obligations shall be charged to Customer at Okta's then current standard hourly rate for services. This section shall not be construed as a waiver of any applicable privilege or protection, including those covering trade secrets and confidential business information.

3.2 Access. All PHI and other information maintained by Okta for Customer will be available to Customer in a time and manner that reasonably allows Customer to comply with the requirements under 45 CFR 164.524 and 164.526. Customer acknowledges that Okta is not required by this BAA to provide any such information directly to any Individual or person other than Customer, and that Okta does not, therefore, expect to maintain documentation of such disclosure as described in 45 CFR 164.528. In the event that Okta does make such disclosure, it shall document the disclosure as would be required for Customer to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR 164.504(e)(2)(ii)(G) and 164.528 and shall provide such documentation to Customer promptly on its request. In the event that a request for an accounting is made directly to Okta, Okta shall, within five (5) business days, forward such request to Customer.

4. Permitted Uses and Disclosures by Okta.

4.1. Functions on Behalf of Customer. Except as otherwise limited in this BAA or other portion of the Agreement, Okta may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Customer as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Customer.

4.2. Data Aggregation Services. Okta may provide Data Aggregation services relating to the Health Care Operations of Customer, to the extent that Okta's services may be deemed Health Care Operations.

4.3. Specific Use and Disclosure Provisions. Except as otherwise limited in this BAA or other portion of the Agreement, Okta may:

a) use PHI for the proper management and administration of Okta or to carry out its legal responsibilities;

b) disclose PHI for the proper management and administration of Okta, provided that disclosures are (i) required by law, or (ii) Okta obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person will notify Okta of any instances of which it is aware in which the confidentiality of the information has been breached; and

c) use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

4.4. De-identification. Okta may de-identify the PHI in accordance with section 164.502(d) of the HIPAA Rules and use, modify and disclose such de-identified data for any legal purpose.

5. **Customer's Obligations.**

5.1. Contact Information. Customer will provide Okta with contact information and will ensure that Customer's contact information remains up to date during the term of this BAA. Contact information must include the name(s) of individual(s) to be contacted, title of individual(s) to be contacted, e-mail address of individual(s) to be contacted, and Customer's name.

5.2. Notification. Customer shall notify Okta of:

a) any limitations(s) in Customer's notice of privacy practices in accordance with 45 CFR 164.520 to the extent that such limitations may affect Okta's use or disclosure of PHI;

b) any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Okta's use or disclosure of PHI; and

c) any restriction to the use or disclosure of PHI that Customer has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Okta's use or disclosure of PHI.

5.3 Operational Obligations. Customer:

a) shall be responsible for implementing appropriate privacy and security safeguards to protect its PHI in compliance with its obligations under HIPAA and retaining the documentation required by the HIPAA Rules for the period of time required by the HIPAA Rules. Without limitation, it is Customer's responsibility to implement privacy and security safeguards in the systems, applications and software Customer controls, configures, or otherwise makes accessible in connection with the Agreement and uploads to the HIPAA Service;

b) warrants that it has obtained any necessary authorizations, consents, and other permissions that may be required under applicable law prior to submitting Customer Data, including without limitation PHI, to the HIPAA Service; and

c) agrees that it will not request Okta to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Customer; provided, however, that this provision shall not be interpreted to restrict Okta from using PHI for Data Aggregation or management and administration and legal responsibilities of Okta, as permitted by this BAA and the Agreement.

d) will make reasonable efforts to limit uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose of the access, use, or disclosure.

e) shall promptly update or delete PHI within the HIPAA Service to reflect any subsequent modifications to, or revocations of, an Individual's consent or authorization governing such PHI.

f) will not agree to or place any restrictions in a Notice of Privacy Practices under 45 CFR 164.520 that conflict with Okta's obligations under this BAA.

6. Term and Termination.

6.1. Term. The term of this BAA shall continue for the term of the Order Form by which Customer purchased access to the HIPAA Service, to store or transmit PHI, and whereby such Order Form is governed by the Agreement to which this BAA is incorporated by reference, and following termination of such Order Form until all PHI is destroyed or returned to Customer or its designee in accordance with Section 6.4 of this BAA.

6.2. Termination by Customer. If Okta materially breaches the terms of this BAA, and Okta has not cured the breach or ended the violation within a reasonable amount of time, then Customer may terminate any related Agreement(s); or if termination is not feasible, Customer shall report the violation to the Secretary.

6.3. Termination by Okta. Upon Okta'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, Customer must take reasonable steps to cure the breach or end the violation. If Customer does not cure the breach or end the violation within a reasonable amount of time, (i) Okta shall terminate this BAA (and the Agreement) upon written notice to Customer or (ii) if termination is not feasible, Okta shall report the violation to the Secretary.

6.4. Effect of Termination. Upon termination of the Agreement, Okta shall make available to Customer its PHI and delete PHI in accordance with the procedures and time periods specified in Okta's relevant retention policies, unless the retention of the PHI is permitted by Okta under applicable laws. If such return or destruction is not feasible, Okta shall extend the protections of this BAA to the PHI and limit further Uses and Disclosures as set forth in Section 4 (Permitted Uses and Disclosures by Okta), for so long as Okta maintains such PHI. This provision shall apply to any subcontractors or agents of Okta who are in possession of Customer's PHI. In the event that Okta determines that destroying the PHI is infeasible, Okta shall promptly provide Customer notification of the conditions that make destruction infeasible. If Okta is required by applicable law to maintain PHI, Customer shall bear the cost of storage of such PHI for as long as storage by Okta is required. Okta will not segregate any PHI from other Customer Data maintained by Okta after termination. Any request for deletion of PHI will include deletion of all Customer Data in the HIPAA Service. For the avoidance of doubt, Okta's obligations to return and/or destroy the PHI as set forth in this Section shall not apply to any PHI which has been de-identified in accordance with the requirements of the HIPAA Rules and Customer acknowledges and agrees that Okta shall be free to continue to use de-identified data without restriction after the termination or expiration of the Agreement.

7. Miscellaneous.

7.1. Notification. Any reports, notifications, or other notice pursuant to this BAA may be made electronically.

7.2 Amendment. Each party agrees to take such action as is reasonably necessary to amend this BAA from time to time for Customer to comply with the requirements of HIPAA as they may be amended; provided, however, that if such an amendment would materially increase the cost of Okta providing Services under the Agreement, Okta shall have the option to terminate the Agreement with thirty (30) days advance notice provided to Customer.

7.3. Survival. The parties' respective rights and obligations under this BAA shall survive the termination of the Agreement.

7.4. Interpretation. Any ambiguity in the Agreement shall be resolved to permit Customer to comply with HIPAA and the Privacy Rule.

7.5. Integration. The Agreement and this BAA constitute the entire and complete understanding of Customer and Okta regarding its subject matter and supersedes all written agreements and understandings between the parties regarding its subject matter.