HIPAA BUSINESS ASSOCIATE ADDENDUM

This HIPAA Business Associate Addendum ("**HIPAA Addendum**") is an addendum to the agreement for Rackspace provided Services to which it is appended or otherwise incorporated ("**Agreement**"). This HIPAA Addendum 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 the HITECH Act and Omnibus Rule, as each may be amended from time to time (collectively, "**HIPAA**"). This HIPAA Addendum is only applicable to HIPAA-Eligible Services; and only if and to the extent that Rackspace is a Business Associate. This HIPAA Addendum prevails over any conflicting terms in the Agreement but does not otherwise modify the Agreement.

1. ADDITIONAL DEFINED TERMS.

"**Business Associate**" means the Rackspace entity providing Services under the Agreement which meets, with respect to Customer and the Services, the definition of a Business Associate under 45 C.F.R. §160.103.

"**CFR**" means the Code of Federal Regulations.

"**HIPAA-Eligible Services**" means the Rackspace Services and the Third Party Infrastructure listed at: https://rackspace.com/information/legal/hipaaeligibleservices (and any successor or related locations designated by Rackspace) subject to any required security configurations applicable to such Services described at such location, as may be updated by Rackspace.

"**HIPAA Breach**" means any Breach or Security Incident, as defined under HIPAA and the HITECH Act, resulting in any actual unauthorized use or disclosure of unsecured PHI caused by Rackspace or its representatives under this BAA.

"**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).

"**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.

"**Protected Health Information**" or "**PHI**" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information received by Business Associate from or on behalf of Customer.

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

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

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

"**Third Party Infrastructure**" means third-party infrastructure (either re-sold through Rackspace, or purchased through any third-party online point-of-sale or provisioning service e.g. the AWS Marketplace or Microsoft Azure Marketplace).

"**Third Party Provider**" means the third-party provider of Third Party Infrastructure.

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 to provide the Services, by this HIPAA Addendum, or as permitted or Required by Law.

2.2. Business Associate agrees to provide those physical, technical and administrative safeguards described in the Agreement including those safeguards and Services selected by Customer and described in a Service Order. If Business Associate agrees as part of this HIPAA Addendum to carry out an obligation of Customer under the Privacy Rule, then Business Associate will comply with the requirements of the Privacy Rule applicable to such obligation.

2.3. Business Associate agrees to mitigate, to the extent commercially reasonable and reasonably practicable, any harmful effect of a HIPAA Breach known to Business Associate.

2.4. Within five Business Days of becoming aware, Business Associate agrees to report to Customer any known HIPAA Breach.

(A) Both parties acknowledge that there are likely to be a significant number of meaningless or unsuccessful attempts to access the Customer Configuration or Services, which make a real-time reporting requirement impractical for both parties. The parties acknowledge that Business Associate's ability to report on system activity, including Security Incidents, is limited by, and to, the Services which Customer has purchased.

(B) Certain Rackspace Services can provide detailed reporting of potential Security Incidents (including those listed below), and Customer is responsible for purchasing, implementing, and monitoring such Services for potential Security Incidents as appropriate based on Customer's use of the Services.

(C) Other than as included with and permitted by those Services that Customer purchases (such as intrusion detection systems or log management) or those procedures separately agreed to in writing (such as configuring SNMP traps on firewall appliances), Business Associate undertakes no obligation to report unsuccessful security incidents or to monitor Customer's Services. Business Associate undertakes no obligation to report network security related incidents which occur on the Rackspace managed network but do not directly involve Customer Data. Where Customer has purchased Services or devices which include reporting on network and system security events, the parties agree that the following are illustrative examples of unsuccessful security incidents which, when they do not result in the unauthorized access, use, disclosure, modification or destruction of PHI need not be reported by Business Associate: pings against network devices, port scans, attempts to log on to a system or database with an invalid password or username, malware.

2.5. Business Associate agrees to obtain from any agent, including a subcontractor to whom it provides Protected Health Information, reasonable assurances that it will adhere to substantially similar restrictions and conditions that apply to Business Associate under this HIPAA Addendum with respect to such information.

2.6. Business Associate shall have no obligation to protect PHI under this Addendum to the extent that Customer creates, receives, maintains, or transmits such PHI outside of the HIPAA-Eligible Services.

2.7. All Protected Health Information maintained by Business Associate for Customer shall be available to Customer in a time and manner that reasonably allows Customer to comply with the requirements under 45 CFR § 164.524. Business Associate shall not be obligated to provide any such information directly to any Individual or person other than Customer.

2.8. All Protected Health Information and other information maintained by Business Associate for Customer will be available to Customer in a time and manner that reasonably allows Customer to comply with the requirements under 45 CFR § 164.526.

2.9. To the extent required by law, and subject to applicable legal privileges, Business Associate agrees to make internal practices, books and records concerning the use and disclosure of PHI received by Business Associate available to the Secretary, in a time and manner designated by the Secretary, for purposes of the

Secretary's determining Customer compliance with the Privacy Rule; provided, however, that time incurred by Business Associate in complying with any such request that exceeds its normal customer service parameters shall be charged to Customer at Business Associate's then current standard hourly rate for professional Services.

2.10. Customer acknowledges that Business Associate is not required by this HIPAA Addendum to make disclosures of Protected Health Information to Individuals or any person other than Customer, and that Business Associate does not, therefore, expect to maintain documentation of such disclosure as described in 45 CFR § 164.528. In the event that Business Associate 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 Customer request. If a request for an accounting is made directly to Business Associate, Business Associate shall, within two Business Days, forward such request to Customer.

3. THIRD PARTY INFRASTRUCTURE. In respect of any Third Party Infrastructure included in the HIPAA-Eligible Services:

3.1. Third Party Providers are not subcontractors or agents of Rackspace.

3.2. Customer represents and warrants that Customer is the owner or authorized user of all Third Party Infrastructure accounts covered by this HIPAA Addendum.

3.3. Business Associate shall require Third Party Providers of HIPAA-Eligible Services to report Security Incidents to Business Associate on no less than a quarterly basis and Breaches of Unsecured PHI on no less than 60 calendar days after discovery of such Breach in a fashion consistent with Business Associates reporting obligations as described in Section 2.4, and unless otherwise included in the Services purchased by Customer, Business Associate undertakes no obligation whatsoever to monitor the Third Party Infrastructure or to report Security Incidents which occur on the Third Party Infrastructure.

3.4. Business Associate undertakes no obligation to report network security related incidents which occur on Third Party Infrastructure, except that Business Associate will report to Customer on a quarterly basis any Security Incidents involving PHI which are reported to Business Associate by Third Party Providers of HIPAA-Eligible Services.

3.5. Customer acknowledges that Business Associate is not required by this HIPAA Addendum to secure, monitor, manage or implement any controls on Third Party Infrastructure.

3.6. Upon termination of this HIPAA Addendum, Business Associate shall require Third Party Providers of HIPAA-Eligible Services, if feasible, to return or destroy all PHI that is still maintained by them in any form, or if such return or destruction is not feasible, extend the protections of this HIPAA Addendum to the PHI and require that Third Party Provider limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. The parties acknowledge that it is not feasible for Business Associate to destroy or return PHI on Third Party Infrastructure upon termination of this HIPAA Addendum, or for Third Party Provider to destroy or return PHI upon termination of this HIPAA Addendum.

4. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE. Except as otherwise limited by this HIPAA Addendum or other portion of the Agreement, Business Associate (and to the extent applicable, Third Party Providers) may use or disclose Protected Health Information 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.

5. SPECIFIC USE AND DISCLOSURE PROVISIONS. Except as otherwise limited in this HIPAA Addendum or other portion of the Agreement, Business Associate (and to the extent applicable, Third Party Providers) may:

5.1. Use Protected Health Information for the proper management and administration of its business or to carry out its legal responsibilities.

5.2. Disclose Protected Health Information for the proper management and administration of its business, provided that disclosures are (i) Required By Law, or (ii) reasonable assurances are obtained 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 Business Associate or Third Party Provider (as applicable) of any instances of which it is aware in which the confidentiality of the information has been breached.

5.3. Use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

6. CUSTOMER OBLIGATIONS.

6.1. Customer shall notify Business Associate of:

(A) Any limitations(s) in Customer notice of privacy practices in accordance with 45 CFR § 164.520 to the extent that such changes may affect Business Associate's or Third Party Provider's (as applicable) use or disclosure of Protected Health Information;

(B) Any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's or Third Party Provider's (as applicable) use or disclosure of Protected Health Information; and

(C) Any restriction to the use or disclosure of Protected Health Information that Customer has agreed in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's or Third Party Provider's (as applicable) use or disclosure of Protected Health Information.

6.2. Customer agrees that Customer will not request that Business Associate or Third Party Provider use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Customer.

6.3. Customer agrees to comply with the security obligations identified in the Agreement, and to implement, purchase, or maintain appropriate safeguards (including security appliances, Services, and practices) as required for Customer to comply with the Security Rule and Privacy Rule as applicable to Customer.

6.4. Customer agrees that Customer shall not provide Business Associate or Third Party Provider with access to unencrypted PHI without Business Associate's prior written permission. Customer must encrypt all PHI stored in or transmitted using the Services in accordance with the Secretary of HHS's Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html, as it may be updated from time to time, and as may be made available on any successor or related site designated by HHS.

7. TERM AND TERMINATION.

7.1. Rackspace or Third Party Provider may add or remove Services or functionality of the Services from the HIPAA-Eligible Services from time to time.

7.2. The term of this HIPAA Addendum shall continue for the term of the Agreement, and following termination of such Agreement until all Protected Health Information is destroyed or returned to Customer or Customer designee.

7.3. If Business Associate materially breaches the terms of this HIPAA Addendum, then Customer may terminate any related Agreement(s) upon ten days written notice to Business Associate provided such breach

is not reasonably capable of being cured. No other termination rights under the Agreement shall apply to breach of this Addendum.

7.4. Upon termination of the Agreement for any reason Business Associate shall destroy all Protected Health Information which remains in Business Associate's possession. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate as well as Business Associate itself. PHI which is located on the Third Party Infrastructure is not considered in Business Associate's possession for the purposes of this Section 7.4. Business Associate shall retain no copies of the Protected Health Information. In the event that Business Associate determines that destroying the Protected Health Information is infeasible, Business Associate shall extend the protections of this HIPAA Addendum to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the destruction infeasible, for so long as Business Associate maintains such Protected Health Information. Customer shall bear the cost of storage of such Protected Health Information for as long as storage by Business Associate is required. This Section does not require Business Associate to segregate any Protected Health Information from other information maintained by Customer on Business Associate's servers and Business Associate may comply with this requirement by returning or destroying all of the information maintained on any Hosted System. By default for Hosted Systems, Rackspace will zero-fill (meaning to format a hard disk by filling available sectors with zeroes) any hard disk drive dedicated to Customer use upon termination of the Service(s). Upon Customer written request, Rackspace shall either physically destroy or multi-pass wipe any hard drive dedicated to Customer use as part of a Hosted System, provided that Rackspace may charge Customer an additional fee at its then current rates for such additional services.

7.5. If Customer request contemporaneously with any termination event or notice, Business Associate will allow Customer to have logical access to any Hosted System (if applicable) for a reasonable period of time following termination as necessary for Customer to retrieve or delete any Protected Health Information subject to prepayment of Fees including fees charged at the then current monthly recurring rate; provided, however, that if the security of Customer servers has been compromised, or the Agreement was terminated for Customer failure to use reasonable security precautions, Rackspace may: (i) provide Customer with restricted access via a dedicated or private link or tunnel to Customer Hosted System or (ii) refuse to allow Customer to have access to Customer Hosted System but shall use reasonable efforts to copy Customer data on to media Customer provide to Rackspace, and will ship the media to Customer at Customer's expense. Rackspace's efforts to copy Customer data onto Customer media shall be billable and prepaid as a professional Service at Rackspace's then current hourly rates.

For Customer	**For Rackspace**
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Job Title: _____	Job Title: _____
Company: _____	Date: _____
Date: _____	