VMWARE BUSINESS ASSOCIATE ADDENDUM

Last updated: 16 August 2022

This Business Associate Addendum ("**BAA**") forms part of the Agreement between VMware, Inc. (**"VMware"**) and the party signing this BAA below ("**Customer**"). This BAA is effective as of the date of last signature (the "**Effective Date**").

1. APPLICABILITY

This BAA will be applicable to Customer's use of the VMware Cloud Service(s) listed in Appendix A (the **"Cloud Service(s)"**) where VMware meets the definition of a Business Associate and Customer uploads PHI (as defined below) to an instance of the Cloud Service provisioned in a data center in the United States.

2. RELATIONSHIP OF PARTIES

For purposes of this BAA, Customer is either a Covered Entity or a Business Associate, and VMware is either a Business Associate or a Subcontractor of the Customer, as such terms are defined under HIPAA.

3. BUSINESS ASSOCIATE RIGHTS AND OBLIGATIONS

3.1. **Limitations on Uses and Disclosures.** VMware will not use or disclose PHI except as permitted or required by this BAA or as Required by Law. Subject to the limitations set forth in this BAA, VMware may use and disclose PHI as necessary in order to provide the Cloud Service.

3.2. VMware may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR 164 if done by Customer, except to the extent that VMware will use or disclose PHI for the management and administration and legal responsibilities of VMware.

3.3. **Permitted Uses and Disclosures.** Subject to the limitations set forth in this BAA, VMware may use PHI if necessary for its proper management and administration or to carry out its legal responsibilities, provided that:

a. Any such disclosure is Required by Law; or

b. (1) VMware obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person; and (2) the person agrees to notify VMware of any instances of which it is aware in which the confidentiality of the PHI has been breached.

3.4. **Data Aggregation.** VMware may use PHI to provide Data Aggregation services to Customer as permitted by 45 C.F.R. 164.504(e)(2)(i)(B) if such services are contemplated as part of the Cloud Service in the applicable Agreement.

3.5. **De-identification.** VMware may use PHI to de-identify PHI in accordance with 45 C.F.R. 164.514(a) if such services are contemplated as part of the Cloud Service in the applicable Agreement. The parties acknowledge and agree that de-identified information is not PHI and is not subject to this BAA.

3.6. **Mitigation.** VMware will mitigate to the extent practicable any harmful effect resulting from a Successful Security Incident involving PHI or any use or disclosure of PHI in violation of the requirements of this BAA, HIPAA, or other applicable law.

3.7. **Subcontractors.** VMware will ensure that any agent, including a Subcontractor, to whom it provides PHI agrees in writing to comply with HIPAA through a business associate or similar agreement with respect to that PHI.

3.8. **Minimum Necessary.** VMware will not request from Customer, use itself, or disclose to its affiliates, subsidiaries, agents, Subcontractors or other third parties, more than the minimum necessary PHI to perform or fulfill a specific function required or permitted hereunder.

3.9. **Incident Reporting.** VMware will report (i) any use or disclosure of PHI not permitted by this BAA, including the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA that compromises the security or privacy of the PHI, and (ii) any Successful Security Incident (each a **"Reportable Incident"**) to Customer promptly, but in no event later

than ten (10) business days, after it is discovered. Such report will be made to the contact person identified at the end of this BAA. VMware will provide the information concerning the Reportable Incident as required by 45 CFR 164.410(c), including VMware's own risk assessment, to determine whether a Breach has occurred. If such information is not available to VMware at the time the Reportable Incident is required to be reported to Customer, VMware will provide that information to Customer promptly as it becomes available. The parties acknowledge that, because VMware does not know the nature of PHI contained in the Cloud Service, it may not be possible for VMware to provide information about the identities of Individuals who may have been impacted, or a description of the type of information that may have been subject to a Reportable Incident. Customer and VMware will mutually determine whether a Breach as defined under 45 CFR 164.410 has occurred. VMware will not be required to report unsuccessful Security Incidents. Both parties acknowledge that there are likely to be a significant number of meaningless or unsuccessful attempts to access the Cloud Service systems, which make a real-time reporting requirement impractical for both parties. The parties acknowledge that VMware's ability to report on system activity, including unsuccessful or attempted Security Incidents, is limited by, and to, the Cloud Service that Customer has purchased.

3.10. Access Requests. Depending on the Cloud Service purchased by Customer, within ten (10) business days of receipt of written notice from Customer, VMware shall make accessible to Customer PHI relating to specified Individuals held by VMware or its agents or Subcontractors in a Designated Record Set in accordance with 45 CFR 164.524. If an Individual requests access to his or her PHI directly from VMware, VMware will, within ten (10) business days of receipt thereof, forward the request to Customer.

3.11. Amendment of PHI. Depending on the Cloud Service purchased by Customer, within ten (10) business days of receipt of a request from Customer, VMware will make accessible to Customer so that Customer may make any requested amendment(s) to PHI held by it or any agent or Subcontractor in a Designated Record Set in accordance with 45 CFR 164.526. In the event any Individual requests an amendment to his or her PHI directly from VMware, VMware will within ten (10) business days of receipt thereof, forward the request to Customer.

3.12. Accounting of Disclosures of PHI. Within ten (10) business days after VMware, its agents or Subcontractors makes any disclosure of PHI for which an accounting may be required under 45 CFR 164.528, VMware will provide in writing to the contact person identified at the end of this BAA, the information related to that disclosure as would be required to respond to a request by an Individual for an accounting in accordance with 45 CFR 164.528. In the event any Individual requests an accounting of disclosures under 45 CFR 164.528(a) directly from VMware, VMware will, within ten (10) business days of receipt thereof, forward the request to Customer. Customer acknowledges and agrees that VMware cannot readily identify which Individuals are identified or what types of PHI are included in Customer Content that Customer or any end user (a) runs on the Cloud Services, (b) causes to interface with the Cloud Services, (c) uploads to the Cloud Services or (d) otherwise transfers, processes, uses or stores in connection with the Cloud Services. Customer will be solely responsible for identifying which Individuals, if any, may have been included in Customer Content that VMware has disclosed and for providing a brief description of the PHI disclosed.

3.13. Books and Records. Upon receipt of written notice from Customer of a request from the Secretary, VMware will make its internal practices, books, and records relating to the use and disclosure of PHI available in a time and manner mutually agreed upon or as required by the Secretary, for purposes of determining compliance with HIPAA. Nothing in this section will waive any applicable privilege or protection, including with respect to trade secrets and confidential commercial information.

3.14. Information Requests. Within fifteen (15) business days of a written request by Customer, VMware will provide Customer with detailed information as may be reasonably requested by Customer from time to time regarding VMware's compliance with its use or disclosure of PHI pursuant to this BAA for the purpose of determining whether VMware has complied with this BAA and HIPAA; provided, however, that (i) disclosure of that information would not violate VMware's confidentiality obligations or reasonable privacy or data security policies and, (ii) Customer will make these requests no more than once in a calendar year unless it is in response to a specific Reportable Incident.

3.15. Documentation. VMware will maintain documentation of its obligations hereunder to the extent and for the period required by HIPAA, including 45 CFR 164.530(j).

4. CUSTOMER OBLIGATIONS

4.1. **Minimum PHI.** Customer will limit disclosure of and access to the minimum amount of PHI, to the minimum number of VMware personnel, for the minimum of amount of time necessary for VMware to accomplish the intended purpose of that use, disclosure, or request, respectively, under the Agreement.

4.2. **Notice of Privacy Practices.** Customer will not agree to any restriction requests or place any restrictions in any notice of privacy practices that would cause VMware to violate this BAA or any applicable law.

4.3. **Restrictions on PHI.** Customer will notify VMware of any restriction on the use or disclosure of PHI that Customer has agreed to or must comply with in accordance with 45 CFR 164.522, to the extent the restriction may affect VMware's use or disclosure of PHI.

4.4. **Change in Permission.** Customer will provide VMware with notice of any changes to or revocation of permission by an Individual to use or disclose PHI, if those changes may affect VMware's permitted uses or disclosures, within a reasonable period of time after Customer becomes aware of those changes to or revocation of permission.

4.5. **Authorizations and Consents**. Customer will obtain any necessary authorizations, consents, and other permissions that may be required by law prior to placing Customer Content, including PHI, in the Cloud Service.

4.6. **Compliance with Policies and Procedures.** Customer will maintain and comply with policies and procedures to avoid the unauthorized or otherwise improper disclosure of PHI to VMware.

4.7. **Security Controls and Safeguards.** Customer will implement appropriate administrative, physical, and technical safeguards to prevent the unauthorized use and disclosure of PHI, and to protect the confidentiality, integrity, and availability of Electronic PHI, as required by HIPAA. Customer will comply with all data protection obligations set forth in the Agreement, including by implementing all required security controls and safeguards. Without limiting the foregoing, Customer will comply with the requirements of 45 CFR 164.308, 164.310, 164.312, and 164.316, as may be amended and interpreted in guidance from time to time. Customer will protect all PHI stored in or transmitted using the Cloud Service in accordance with the Secretary of HHS's "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals", available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.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. Customer will not provide, create, receive, maintain, or transmit any PHI as part of the Cloud Service that is not encrypted in accordance with the foregoing, will utilize the highest level of audit logging in connection with VMware's use of the Cloud Service, and will maintain the maximum retention of logs in connection with VMWare's use of PHI.

4.8. Customer will perform its responsibilities under the Agreement, including, without limitation, obligations relating to provisioning, connectivity, configuration, encryption, security, data protection, data restoration, monitoring, incident, and problem management, and change management.

4.9. Customer will not request VMware to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR 164 if done by the Customer, except to the extent that VMware will use or disclose PHI for the management and administration and legal responsibilities of the VMware.

5. SECURITY OF PROTECTED HEALTH INFORMATION

5.1. VMware will implement appropriate administrative, physical, and technical safeguards for the Cloud Service to prevent the unauthorized use and disclosure of PHI, and to protect the confidentiality, integrity, and availability of Electronic PHI, as required by HIPAA. Without limiting the foregoing, VMware will comply with the requirements of 45 CFR 164.308, 164.310, 164.312, and 164.316, as may be amended and interpreted in guidance from time to time.

5.2. VMware will conduct periodic reviews of its security safeguards to ensure they are appropriate and operating as intended.

6. TERM AND TERMINATION.

6.1. **Term.** The term of this BAA will continue for so long as the applicable Agreement remains in effect, except that (i) Section 7(c) (Return and Destruction of PHI) will survive after the termination of the applicable Agreement for as long as VMware retains any PHI; and (ii) any provision that by its nature survives termination will so survive.

6.2. **Period to Cure.** Upon Customer's determination that VMware has violated or breached a material term of this BAA, Customer shall provide an opportunity for VMware to cure the breach or end the violation, and Customer may terminate this BAA if VMware does not cure the breach or end the violation within a reasonable period.

6.3. **Return and Destruction of PHI.** Except as provided in this Section 7(c), upon termination of the applicable Agreement for any reason, VMware will return to Customer or destroy all PHI in its possession or that of its Subcontractors or agents consistent with the applicable Agreement. If returning or destroying the PHI is impractical upon termination of the applicable Agreement, VMware will extend the protections of this BAA to such PHI, and limit further uses and disclosures of it to those purposes that make the return or destruction infeasible, for so long as VMware or its agents or Subcontractors store such PHI. Customer will bear the cost of such storage for as long as it is required. This Section 7(c) does not require VMware to segregate any PHI from other information maintained by Customer on VMware's systems and VMware may comply with this requirement by returning or destroying all of the information maintained in its systems by Customer.

7. Miscellaneous

7.1. The parties will take action as is necessary to negotiate in good faith to amend this BAA from time to time to comply with the requirements of HIPAA; provided, however, that if any amendment of HIPAA or guideline from the Department of Health and Human Services would materially increase the cost of VMware providing the Cloud Service under the applicable Agreement, then VMware will have the option to terminate the applicable Order on the earlier of thirty (30) days advance notice or the date such amendment or guideline becomes effective. In the event of that termination, VMware will refund any prepaid fees, pro-rated for the remainder of the applicable Order, and less any discounts that are not earned as of the effective date of termination.

7.2. A reference in this BAA to a section in HIPAA means the section as in effect or as amended, and as of its effective date.

7.3. Any ambiguity in this BAA shall be resolved to permit compliance with HIPAA.

7.4. The terms and conditions of this BAA shall override and control any conflicting term or condition of the applicable Agreement. All non-conflicting terms and conditions of the applicable Agreement remain in full force and effect.

7.5. **Relationship of Parties.** It is expressly agreed that VMware, its divisions, and its affiliates, including its employees and Subcontractors, are providing all or part of the Cloud Service under this BAA as independent contractors for Customer. Neither VMware nor of its affiliates, officers, directors, employees, or Subcontractors is an employee or agent of Customer. Nothing in this BAA will be construed to create (i) a partnership, joint venture, or other joint business relationship between the parties or any of their affiliates, or (ii) an agency relationship for purposes of HIPAA.

8. DEFINITIONS

Agreement means the written or electronic agreement between Customer and VMware for the provision of the Cloud Services to Customer.

Breach has the same meaning as the term "Breach" in 45 CFR 164.402.

HIPAA means the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act") and the federal regulations published at 45 CFR parts 160 and 164.

Individual has the same meaning as the term "Individual" in 45 CFR 160.103 and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g) or other applicable law.

Protected Health Information or **PHI** has the same meaning as that term is defined in 45 CFR 160.103, but is limited to information created, received, maintained, or transmitted by VMware on behalf of Customer and included in any Customer Content.

Required by Law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Secure means to render unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of the HITECH Act.

Subcontractor means a person to whom VMware delegates a function, activity, or service that creates, receives, maintains, or transmits PHI on behalf of VMware.

Successful Security Incident means any Security Incident (as defined in 45 CFR 164.304) that results in the unauthorized use, access, disclosure, modification, or destruction of Electronic PHI.

All capitalized terms used in this BAA and not defined in this BAA or in the applicable Agreement will have the same meaning as those terms are used or defined in HIPAA.

By signing below, each party agrees to the terms of this BAA. Each of the individuals signing this BAA represents that they have the authority to bind their respective party to its terms.

VMWARE, INC.

Signature _____

Name _____

Title _____

Date _____

_____

CUSTOMER

Signature _____

Name _____

Title _____

Date _____

Privacy or Security Contact Person

(for the purposes of notification under Section 4(i) (Incident Reporting)

Name _____

Title _____

Date _____

Appendix A – Covered Cloud Services

1. VMC on AWS
2. VMware Cloud Disaster Recovery (VCDR)