

HIPAA Business Associate Agreement

If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Data or FastTrack Data, execution of a license agreement that includes the Online Services Terms (“Agreement”) will incorporate the terms of this HIPAA Business Associate Agreement (“BAA”) into that Agreement. If there is any conflict between a provision in this BAA and a provision in the Agreement, this BAA will control.

1. Definitions.

Except as otherwise defined in this BAA, capitalized terms shall have the definitions set forth in HIPAA, and if not defined by HIPAA, such terms shall have the definitions set forth in the Agreement.

“Breach Notification Rule” means the Breach Notification for Unsecured Protected Health Information Final Rule.

“Business Associate” shall have the same meaning as the term “business associate” in 45 CFR § 160.103 of HIPAA.

“Covered Entity” shall have the same meaning as the term “covered entity” in 45 CFR § 160.103 of HIPAA.

“Customer”, for this BAA only, means Customer and its Affiliates.

“FastTrack Data” means all data, including all text, sound, video, or image files, and software, that are provided to “VENDOR” by or on behalf of Customer for “VENDOR”’s performance of the FastTrack Services.

“FastTrack Services” means the onboarding and migration services for Office 365 Services specified as being in scope for this BAA on the FastTrack Center BAA site at <http://aka.ms/FastTrackBAA> (or successor site) that are provided to Customer by “VENDOR” in connection with Customer’s subscription for Office 365 Services, excluding services that are performed using third-party software or software that is not hosted by “VENDOR”.

“HIPAA” collectively means the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations, including the Privacy Rule, the Breach Notification Rule, and the Security Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act and by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

““VENDOR” Online Services”, for this BAA only, means Office 365 Services, “VENDOR” Azure Core Services, “VENDOR” Dynamics 365 Core Services, “VENDOR” Intune Online Services, “VENDOR” Power Platform Core Services, and/or “VENDOR” Cloud App Security, each as defined in the “Data Protection Terms” section of the Online Services Terms incorporated into the Agreement; “VENDOR” Healthcare Bot; and any additional Azure online services and U.S. Government online services listed as in scope for this BAA on the “VENDOR” Trust Center at <https://www.”VENDOR”.com/en-us/trustcenter/Compliance/HIPAA> (or successor site); excluding Previews.

“Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information.

“Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103 of HIPAA, provided that it is limited to such protected health information that is

received by "VENDOR" from, or created, received, maintained, or transmitted by "VENDOR" on behalf of, Customer (a) through the use of the "VENDOR" Online Services or (b) for "VENDOR"'s performance of the FastTrack Services.

"Security Rule" means the Security Standards for the Protection of Electronic Protected Health Information.

2. Permitted Uses and Disclosures of Protected Health Information.

- a. Performance of the Agreement for "VENDOR" Online Services.** Except as otherwise limited in this BAA, "VENDOR" may Use and Disclose Protected Health Information for, or on behalf of, Customer as specified in the Agreement; provided that any such Use or Disclosure would not violate HIPAA if done by Customer, unless expressly permitted under paragraph b of this Section.
- b. Management, Administration, and Legal Responsibilities.** Except as otherwise limited in this BAA, "VENDOR" may Use and Disclose Protected Health Information for the proper management and administration of "VENDOR" and/or to carry out the legal responsibilities of "VENDOR", provided that any Disclosure may occur only if: (1) Required by Law; or (2) "VENDOR" obtains written reasonable assurances 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 purpose for which it was Disclosed to the person, and the person notifies "VENDOR" of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.

3. Responsibilities of the Parties with Respect to Protected Health Information.

- a. "VENDOR"'s Responsibilities.** To the extent "VENDOR" is acting as a Business Associate, "VENDOR" agrees to the following:
 - (i) Limitations on Use and Disclosure.** "VENDOR" shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Agreement and/or this BAA or as otherwise Required by Law. "VENDOR" shall not disclose, capture, maintain, scan, index, transmit, share or Use Protected Health Information for any activity not authorized under the Agreement and/or this BAA. Neither "VENDOR" Online Services nor FastTrack Services shall use Protected Health Information for any advertising, Marketing or other commercial purpose of "VENDOR" or any third party. "VENDOR" shall not violate the HIPAA prohibition on the sale of Protected Health Information. "VENDOR" shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.
 - (ii) Safeguards.** "VENDOR" shall: (1) use reasonable and appropriate safeguards to prevent inappropriate Use and Disclosure of Protected Health Information other than as provided for in this BAA; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.
 - (iii) Reporting.** "VENDOR" shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which "VENDOR" becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no

further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer's Unsecured Protected Health Information that "VENDOR" may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made without unreasonable delay, but in no event more than five (5) business days after "VENDOR"'s determination of a Breach. Taking into account the level of risk reasonably likely to be presented by the Use, Disclosure, Security Incident, or Breach, the timing of other reporting will be made consistent with "VENDOR"'s and Customer's legal obligations.

For purposes of this Section, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on "VENDOR"'s firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information. Notification(s) under this Section, if any, will be delivered to contacts identified by Customer pursuant to Section 3b(ii) (Contact Information for Notices) of this BAA by any means "VENDOR" selects, including through e-mail. "VENDOR"'s obligation to report under this Section is not and will not be construed as an acknowledgement by "VENDOR" of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

- (iv) Subcontractors.** In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, "VENDOR" shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of "VENDOR" to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to "VENDOR" 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. "VENDOR" remains responsible for its Subcontractors' compliance with obligations in this BAA.
- (v) Disclosure to the Secretary.** "VENDOR" shall make available its internal practices, records, and books relating to the Use and/or Disclosure of Protected Health Information received from Customer to the Secretary of the Department of Health and Human Services for purposes of determining Customer's compliance with HIPAA, subject to attorney-client and other applicable legal privileges. "VENDOR" shall respond to any such request from the Secretary in accordance with the Section titled "Disclosure of Customer Data" in the Agreement.
- (vi) Access.** If "VENDOR" maintains Protected Health Information in a Designated Record Set for Customer, then "VENDOR", at the request of Customer, shall within fifteen (15) days make access to such Protected Health Information available to Customer in accordance with 45 CFR § 164.524 of the Privacy Rule.
- (vii) Amendment.** If "VENDOR" maintains Protected Health Information in a Designated Record Set for Customer, then "VENDOR", at the request of Customer, shall within fifteen (15) days make available such Protected Health Information to Customer for amendment and incorporate any reasonably requested amendment in the Protected Health Information in accordance with 45 CFR § 164.526 of the Privacy Rule.
- (viii) Accounting of Disclosure.** "VENDOR", at the request of Customer, shall within fifteen (15) days make available to Customer such information relating to Disclosures made by

“VENDOR” as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.

- (ix) **Performance of a Covered Entity’s Obligations.** To the extent “VENDOR” is to carry out a Covered Entity obligation under the Privacy Rule, “VENDOR” shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.

b. Customer Responsibilities.

- (i) **No Impermissible Requests.** Customer shall not request “VENDOR” to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).
- (ii) **Contact Information for Notices.** Customer hereby agrees that any reports, notification, or other notice by “VENDOR” pursuant to this BAA may be made electronically. Customer shall provide contact information as follows (or as “VENDOR” may specify from time to time): (1) the Azure Security Center for “VENDOR” Azure Core Services, (2) MSO-HIPAA@“VENDOR”.com for other Azure or U.S. Government online services in scope for this BAA, and (3) the Message Center in the Admin Center for other “VENDOR” Online Services. Contact information (a) for “VENDOR” Azure Core Services must include the security contact information required on the Azure Security Center, (b) for other Azure or U.S. Government online services in scope for this BAA must include name of individual(s) to be contacted, title of individual(s) to be contacted, e-mail address of individual(s) to be contacted, name of Customer organization, and, if available, Customer’s contract number, subscriber identification number, and “VENDOR” Online Direct Routing Domain (MODRD) (e.g. “contoso.on”VENDOR”.com”), and (c) for other “VENDOR” Online Services must include information required for the Message Center Privacy reader role in the Admin Center. Customer shall ensure that such contact information remains up to date during the term of this BAA. Failure to submit and maintain as current the aforementioned contact information may delay “VENDOR”’s ability to provide Breach notification under this BAA.
- (iii) **Safeguards and Appropriate Use of Protected Health Information.** Customer is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Customer’s obligation to:
 - 1) Not include Protected Health Information in: (1) information Customer submits to technical support personnel through a technical support request or to community support forums; and (2) Customer’s address book or directory information. In addition, “VENDOR” does not act as, or have the obligations of, a Business Associate under HIPAA with respect to Customer Data or FastTrack Data once it is sent to or from Customer outside “VENDOR” Online Services or FastTrack Services over the public Internet, or if Customer fails to follow applicable instructions regarding physical media transported by a common carrier.
 - 2) Implement privacy and security safeguards in the systems, applications, and software Customer controls, configures, and uploads into the “VENDOR” Online Services or uses in connection with the FastTrack Services.

4. *Applicability of BAA.*

This BAA is applicable to “VENDOR” Online Services and FastTrack Services. “VENDOR” may, from time to time, (a) include additional “VENDOR” online services on the “VENDOR” Trust Center and/or in the “Data Protection Terms” section of the Online Services Terms incorporated into the Agreement or additional FastTrack Services on the FastTrack Center BAA site, and (b) update the definition of “VENDOR” Online Services and FastTrack Services in this BAA accordingly, and such updated definitions will apply to Customer without additional action by Customer. It is Customer’s obligation to not store or process in an online service, or provide to “VENDOR” for performance of a professional service, protected health information (as that term is defined in 45 CFR § 160.103 of HIPAA) until this BAA is effective as to the applicable service.

5. *Term and Termination.*

- a. Term.** This BAA shall continue in effect until the earlier of (1) termination by a Party for breach as set forth in Section 5b, below, or (2) expiration of Customer’s Agreement.
- b. Termination for Breach.** Upon written notice, either Party immediately may terminate the Agreement and this BAA if the other Party is in material breach or default of any obligation in this BAA. Either party may provide the other a thirty (30) calendar day period to cure a material breach or default within such written notice.
- c. Return, Destruction, or Retention of Protected Health Information Upon Termination.** Upon expiration or termination of this BAA, “VENDOR” shall return or destroy all Protected Health Information in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Agreement. If it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this BAA, then “VENDOR” shall extend the protections of this BAA, without limitation, to such Protected Health Information and limit any further Use or Disclosure of the Protected Health Information to those purposes that make the return or destruction infeasible for the duration of the retention of the Protected Health Information.

6. *Miscellaneous.*

- a. Interpretation.** The Parties intend that this BAA be interpreted consistently with their intent to comply with HIPAA and other applicable federal and state law. Except where this BAA conflicts with the Agreement, all other terms and conditions of the Agreement remain unchanged. Any captions or headings in this BAA are for the convenience of the Parties and shall not affect the interpretation of this BAA.
- b. BAAs; Waiver.** This BAA may not be modified or amended except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, as a bar to, or as a waiver of any right or remedy as to subsequent events.
- c. No Third-Party Beneficiaries.** Nothing express or implied in this BAA is intended to confer, nor shall anything in this BAA confer, upon any person other than the Parties, and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

- d. Severability.** In the event that any provision of this BAA is found to be invalid or unenforceable, the remainder of this BAA shall not be affected thereby, but rather the remainder of this BAA shall be enforced to the greatest extent permitted by law.
- e. No Agency Relationship.** It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Customer and “VENDOR” under HIPAA or the Privacy Rule, Security Rule, or Breach Notification Rule. No terms or conditions contained in this BAA shall be construed to make or render “VENDOR” an agent of Customer.