Microsoft Online Services HIPAA Business Associate

The Microsoft Online Services provided to Customer require Microsoft to host Customer Data that may contain Protected Health Information. Customer is a Covered Entity or a Business Associate. To the extent Microsoft creates, receives, maintains, or transmits Protected Health Information, Microsoft is a Business Associate of Customer. As such, HIPAA requires Microsoft and Customer to comply with additional obligations under the Privacy Rule, Breach Notification Rule, and Security Rule that relate to the Use, access, and Disclosure of Protected Health Information. The Agreement is amended by adding the following:

1. Definitions

Except as otherwise defined in this Amendment, any and all capitalized terms shall have the definitions set forth in HIPAA, and Customer's 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" means the customer identified on the signature form.

"Dynamics CRM Online Services" means Dynamics CRM Online services made available through volume licensing or the Microsoft online services portal, excluding Dynamics CRM for supported devices, which includes but it is not limited to Dynamics CRM Online services for tablets and/or smartphones and any separately branded service made available with or connected to Dynamics CRM Online such as Microsoft Social Engagement, Parature, from Microsoft, and Microsoft Dynamics Marketing .

"HIPAA" collectively means the administrative simplification provision of the c 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.

"Microsoft Azure Core Services" means the following features of Microsoft Azure Services: Cloud Services (web and worker roles), Virtual Machines (including with SQL Server), Storage (Blobs, Tables, Queues), Virtual Network, Traffic Manager, Batch, Web Sites, BizTalk Services, Media Services, Mobile Services, Service Bus, Notification Hub, Workflow Manager, Express Route, Scheduler, Multi-Factor Authentication, Active Directory, Rights Management Service, SQL Database, HDInsight and any other features identified as included on the Microsoft Azure Trust Center.

"Microsoft Intune Online Services" means the cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune

such as Mobile Device Management for Office 365. It does not include any on-premises software made available with a Microsoft Intune.

"Microsoft Power BI Services" means the cloud service portion of Microsoft Power BI offered as a standalone service or as included in an Office 365 branded plan or suite, but excluding data catalog functionality, the Power BI mobile applications, and Power BI Desktop.

"Microsoft Online Services" for this Amendment only, means Dynamics CRM Online Services, Office 365 Services, Microsoft Azure Core Services, Microsoft Intune Online Services, and/or Microsoft Power BI Services.

"Office 365 Services" means the following services, each as a standalone service or as included in an Office 365-branded plan or suite: Exchange Online, Exchange Online Archiving, Exchange Online Protection, Advanced Threat Protection, SharePoint Online, OneDrive for Business, Project Online, Skype for Business Online, Sway, Office Online, and Yammer Enterprise. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded "for Office 365."

"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 Microsoft from, or created, received, maintained, or transmitted by Microsoft on behalf of, Customer.

"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 Microsoft Online Services.** Except as otherwise limited in this Amendment, Microsoft 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 Amendment, Microsoft may Use and Disclose Protected Health Information for the proper management and administration of Microsoft and/or to carry out the legal responsibilities of Microsoft, provided that any Disclosure may occur only if: (1) Required by Law; or (2) Microsoft 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 Microsoft 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. **Microsoft's Responsibilities.** To the extent Microsoft is acting as a Business Associate, Microsoft agrees to the following:

(i) **Limitations on Use and Disclosure.** Microsoft shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Agreement and/or this Amendment or as otherwise Required by Law; Microsoft 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 Amendment. Microsoft Online Services shall not use Protected Health Information for any advertising, Marketing or other commercial purpose of Microsoft or any third party. Microsoft shall not violate the HIPAA prohibition on the sale of Protected Health Information. Microsoft 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.** Microsoft shall: (1) use reasonable and appropriate safeguards to prevent inappropriate Use and Disclosure of Protected Health Information other than as provided for in this Amendment; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.

(iii) **Reporting.** Microsoft shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this Amendment of which Microsoft 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 Microsoft 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 thirty (30) calendar days after discovery 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 Microsoft's and Customer's legal obligations.

For purposes of this Section, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on Microsoft'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 Amendment by any means Microsoft selects, including through e - mail. Microsoft's obligation to report under this Section is not and will not be construed as an acknowledgement by Microsoft 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, Microsoft shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Microsoft to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Microsoft 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. Microsoft remains responsible for its subcontractors' compliance with obligations in this Amendment.

(v) **Disclosure to the Secretary.** Microsoft 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. Microsoft 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 Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, 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 Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, at the request of Customer, shall 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.** Microsoft, at the request of Customer, shall within fifteen (15) days make available to Customer such information relating to Disclosures made by Microsoft 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 Microsoft is to carry out a Covered Entity obligation under the Privacy Rule, Microsoft 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 Microsoft 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 Microsoft pursuant to this Amendment may be made electronically. Customer shall provide contact information to MSO-HIPAA@microsoft.com or such other location or method of updating contact information as Microsoft may specify from time to time and shall ensure that Customer's contact information remains up to date during the term of this Amendment. Contact information must include name of individual(s) to be contacted, title of individuals(s) to be contacted, e-mail address of individual(s) to be contacted, name of Customer organization, and, if available, either contract number or subscriber identification number.

(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, Microsoft does not act as, or have the obligations of, a Business Associate under HIPAA with respect to Customer Data once it is sent to or from Customer outside Microsoft Online Services over the public Internet.

2) Implement privacy and security safeguards in the systems, applications, and software Customer controls, configures, and uploads into the Microsoft Online Services.

4. Applicability of Amendment.

As of the effective date of this Amendment, this Amendment is applicable to Microsoft Online Services. Microsoft may, from time to time, update the definition of this Amendment with respect to other current or future Microsoft online services. Any such updated definitions will apply to Customer without additional action by Customer. Customer acknowledges that this Amendment is not effective as to an applicable Microsoft online service until Microsoft notifies Customer this Amendment is effective as specified in this Section 4. It is Customer's obligation to not store or process Protected Health Information in a Microsoft online service until this Amendment is effective as to the applicable service.

5. Term and Termination.

a. **Term.** This Amendment shall continue in effect except in case of termination by a Party for breach as set forth in Section 5b .

b. **Termination for Breach.** Upon written notice, either Party immediately may terminate the Agreement and this Amendment if the other Party is in material breach or default of any obligation in this Amendment. 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 Amendment, Microsoft shall return or destroy all Protected Health Information in its possession, if it is feasible to do so . If it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this Amendment, then Microsoft shall extend the protections of this Amendment, 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 Amendment be interpreted consistently with their intent to comply with HIPAA and other applicable federal and state law. Except

where this Amendment conflicts with the Agreement, all other terms of the Agreement remain unchanged. The Parties agree that, in the event an inconsistency exists between the Agreement and this Amendment, the provisions of this Amendment will control to the extent of such inconsistency. Any captions or headings in this Amendment are for the convenience of the Parties and shall not affect the interpretation of this Amendment.

b. **Amendments; Waiver.** This Amendment 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 Amendment is intended to confer, nor shall anything in this Amendment 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. **Counterparts.** This Amendment may be executed in counterparts, each of which shall be deemed an original.

e. **Severability.** In the event that any provision of this Amendment is found to be invalid or unenforceable, the remainder of this Amendment shall not be affected thereby, but rather the remainder of this Amendment shall be enforced to the greatest extent permitted by law.

f. **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 Microsoft under HIPAA or the Privacy Rule, Security Rule, or Breach Notification Rule. No terms contained in this Amendment shall be construed to make or render Microsoft an agent of Customer.