Microsoft Volume Licensing

Microsoft Online Subscription Agreement/Open Program License Agreement

Amendment for HIPAA and HITECH Act

Amendment ID MOS13

To be valid, Customer must have accepted this Amendment as set forth in the Microsoft Online Services portal.

This amendment ("Amendment") is between the customer entity ("Customer") and the Microsoft entity ("Microsoft") who are party to either (a) the Microsoft Online Subscription Agreement or (b) an Open Program license agreement, as applicable,(the "Agreement") under which Customer has purchased Microsoft Online Services, and supplements the Agreement.

The Microsoft Online Services provided to Customer require Microsoft to host Customer Data that may contain Protected Health Information. The HITECH Act and HIPAA require Microsoft and Customer, as a Business Associate and Covered Entity, respectively, to comply with additional Privacy Standards and Security Standards that relate to the use, access, and disclosure of Protected Health Information.

The terms and conditions in this Amendment supersede any conflicting terms and conditions in the Agreement. The parties amend the Agreement with the following:

1. *Definitions.*

Except as otherwise defined in this Amendment, any and all capitalized terms shall have the definitions set forth in HIPAA, the HITECH Act, and Covered Entity's Agreement for Microsoft Online Services.

"Business Associate" refers to Microsoft for purposes of this Amendment.

"Covered Entity" means Customer.

"Customer Data" means all data, including all text, sound, software or image files that are provided to Business Associate by, or on behalf of, Covered Entity through Covered Entity's use of the Microsoft Online Services.

"Dynamics CRM Online Services" means Dynamics CRM Online volume licensing SKUs such as DynCRMOnIn ALNG SubsVL MVL PerUsr (DSD-00001). Dynamics CRM Online Services does not include the Dynamics CRM Mobile service.

"HIPAA" 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 Standards for Privacy of Individually Identifiable Health Information and the Security Rule.

"The HITECH Act" means the Health Information Technology for Economic and Clinical Health Act enacted by the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and its implementing regulations.

"Microsoft Online Services" for this amendment only, means Office 365 Services and/or Microsoft Dynamics CRM Online Services.

"Office 365 Services" means (a) Exchange Online, Exchange Online Archiving, SharePoint Online, Lync Online, and Office Web Apps included in Office 365 Enterprise Plans E1, E2, E3, E4, K1, and K2; Office 365 Academic Plans A2, A3, and A4; Office 365 Midsize Business; Office 365 Small Business; and Office 365 Small Business Premium; and (b) Exchange Online Plans 1, 2, Basic, and Kiosk; SharePoint Online Plans 1, 2, and Kiosk; Office Web Apps Plans 1 and 2; and Lync Online Plans 1, 2, and 3. Office 365 Services do not include Office 365 ProPlus or any separately branded service made available with an Office 365-branded plan or suite.

"Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103 provided that it is limited to such protected health information that is received by Business Associate from, received by Business Associate on behalf of, or created by Business Associate on behalf of Covered Entity.

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

1. Permitted Uses and Disclosures of Protected Health Information.

a. Performance of the Agreement. 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.

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.

2. 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; provided that any such Use or Disclosure would not violate HIPAA if done by Customer, unless expressly permitted for Business Associates under HIPAA. 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.

(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.

(vi) Access. If Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, at the request of Customer, shall 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 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 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.

3. Applicability of Amendment.

As of the effective date of this Amendment, this Amendment is applicable to Microsoft Online Services. At such time as Microsoft is willing to enter into the terms of this Amendment with respect to other current or future Microsoft online services, Microsoft will notify Customer of the effective date that this Amendment will be applicable to such other Microsoft online services. Subsequent to the effective date identified in Microsoft's notice, and provided Customer has by that date entered into an agreement for such other Microsoft online services, this Amendment will apply to Customer's other Microsoft online services 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 on or after the date this Amendment is effective as to the applicable service.

4. Term and Termination.

a. Term. This Amendment 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 Enrollment

b. Termination for Breach. Either Party immediately may terminate the Agreement if the other Party is in material breach or default of any obligation in this Amendment that is not cured within thirty (30) calendar days written notice of such breach or default.

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, and as set forth in the applicable termination provisions of the Product Use Rights and/or Enrollment. If Microsoft determines that 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.

5. 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 and conditions 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.