

Microsoft Online Subscription 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 the Microsoft Online Subscription Agreement (“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 Office 365 Plans E1, E2, E3, E4, P1, K1, and K2; Exchange Online Plan 1, Plan 2, and Kiosk; Exchange Online Archiving; SharePoint Online Plans 1 and 2; Office Web Apps Plans 1 and 2; and Lync Online Plans 1 and 2.

“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.

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, Business Associate may use and disclose Protected Health Information for, or on behalf of, Covered Entity as specified in the Agreement for Microsoft Online Services.

b. Management, Administration, and Legal Responsibilities. Except as otherwise limited in this Amendment, Business Associate may use and disclose Protected Health Information for the proper management and administration of Business Associate and/or to carry out the legal responsibilities of Business Associate, provided that any disclosure may occur only if: (1) Required by Law; or (2) Business Associate 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 Business Associate of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.

c. Data Aggregation. Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity if Business Associate determines that Data Aggregation, as it relates to the health care operations of Covered Entity, is necessary to provide or improve the Microsoft Online Services for the benefit of Covered Entity.

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

a. Responsibilities of Business Associate. To the extent Business Associate is acting as a business associate as defined by HIPAA, Business Associate agrees to the following:

(i) Limitations on Use and Disclosure. Business Associate shall use and/or disclose the Protected Health Information only as permitted or required by the Agreement for Microsoft Online Services or this Amendment or as otherwise Required by Law; provided that any such use or disclosure would not violate HIPAA if done by Covered Entity unless expressly permitted for business associates under HIPAA and/or the HITECH Act.

(ii) Safeguards. Business Associate shall use reasonable and appropriate: (1) safeguards to prevent inappropriate use and disclosure of Protected Health Information other than as provided for in this Amendment; and (2) administrative, physical, and technical safeguards that appropriately protects the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity.

(iii) Reporting. Business Associate shall report to Covered Entity: (1) any use and/or disclosure of Protected Health Information that is not permitted or required by this Amendment of which Business Associate 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 Covered Entity’s Unsecured Protected Health Information that Business Associate may discover. 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, incident, or breach, the timing of other reporting will be made consistent with Business Associate’s and Covered Entity’s legal obligations.

For purposes of this Section, “Unsuccessful Security Incidents” means, without limitation, pings and other broadcast attacks on Business Associate’s firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use or

disclosure of Protected Health Information. Notification(s) under this Section, if any, will be delivered to contacts identified by Covered Entity pursuant to Section 3b(ii) (Contact Information for Notices) of this Amendment by any means Business Associate selects, including via email. Business Associate's obligation to report under this Section is not and will not be construed as an acknowledgement by Business Associate of any fault or liability with respect to any use, disclosure, Security Incident, or Breach.

(iv) Subcontractors. Business Associate shall require all of its subcontractors and agents to whom it provides Protected Health Information to agree in writing to: (1) the same restrictions and conditions that apply to Business Associate with respect to such Protected Health Information; and (2) implement reasonable and appropriate safeguards to protect Protected Health Information.

(v) Disclosure to the Secretary. Business Associate shall make available its internal practices, records, and books, including Protected Health Information, relating to the use and/or disclosure of Protected Health Information received from Covered Entity to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with HIPAA, subject to attorney-client and other applicable legal privileges.

(vi) Access. If Business Associate maintains Protected Health Information in a Designated Record Set for Covered Entity, Business Associate shall make access to such Protected Health Information available to Covered Entity in accordance with HIPAA and the HITECH Act.

(vii) Amendment. If Business Associate maintains Protected Health Information in a Designated Record Set for Covered Entity, Business Associate shall make available such Protected Health Information to Covered Entity for amendment and incorporate any such amendment in the Protected Health Information as may be reasonably requested by Covered Entity in accordance with HIPAA and the HITECH Act.

(viii) Accounting of Disclosure. Business Associate shall make available to Covered Entity such information relating to disclosures made by Business Associate as required for Covered Entity to make any requested accounting of disclosures in accordance with HIPAA and the HITECH Act.

(ix) HITECH Act Compliance. With respect to any business associate functions, Business Associate shall comply with the provisions of the Security Rule that are made applicable to business associates by the HITECH Act, including the administrative, physical, and technical standards of the Security Rule and the requirements to maintain policies, procedures, and documentation of security activities.

b. Responsibilities of Covered Entity.

(i) No Impermissible Requests. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under HIPAA or the HITECH Act if done by Covered Entity.

(ii) Contact Information for Notices. This Section constitutes Covered Entity's agreement to receive electronic notification reports in order for Covered Entity to timely receive notifications contemplated by Section 3a(iii) (Reporting) or other notices relevant to this Amendment. In the event such notifications are required, Business Associate may notify the Covered Entity representative who agreed to this Amendment or any other Covered Entity personnel designated as Covered Entity's administrators for purposes of the Microsoft Online Services as reflected in the administrative portal for the services. To facilitate such notifications, Covered Entity shall ensure that contact information for Covered Entity's Microsoft Online Services administrators remains up to date during the term of this Amendment.

(iii) Appropriate Use of Protected Health Information. Covered Entity is responsible for implementing appropriate privacy and security safeguards in order to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Covered Entity's obligation not to include Protected Health Information in: (1) information Covered Entity submits to technical support personnel or Microsoft Online community support forums; and (2) Covered Entity'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 Covered Entity outside the Microsoft Online service over the public Internet.

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 4(b), below, or (2) subject to Section 5(c) Amendments, below, expiration of Covered Entity's Agreement for Microsoft Online Services.

b. Termination for Breach. Either Party may immediately terminate the Agreement for Microsoft Online Services 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, Business Associate 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 Online Services Use Rights and/or Agreement for the Microsoft Online Services. If Business Associate determines that it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this Amendment, then Business Associate 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. HITECH Act Requirements. The Parties agree that the provisions under the HITECH Act that are required by law to be incorporated into this Amendment are hereby incorporated into this Amendment.

b. Interpretation. The Parties intend that this Amendment be interpreted consistently with their intent to comply with HIPAA, the HITECH Act, and other applicable federal and state law. Except where this Amendment conflicts with the Agreement for Microsoft Online Services, all other terms and conditions of the Agreement for Microsoft Online Services remain unchanged. The Parties agree that, in the event an inconsistency exists between the Agreement for Microsoft Online Services 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.

c. Amendments.

(i.) During Committed Term. During Covered Entity's committed term for the Microsoft Online Services, this Amendment may not be modified or amended except in a writing duly signed by authorized representatives of the Parties.

(ii.) Renewal Term. Business Associate may update this Amendment by notifying the Covered Entity representative who agreed to this Amendment (or any other Covered Entity personnel designated as Covered Entity's administrators for purposes of the Microsoft Online Services as reflected in the administrative portal for the services) prior to the end of Covered Entity's committed term, and the updated Amendment shall apply to Covered Entity's use of the Microsoft Online Services after the renewal date.

d. Waiver. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

e. 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.

f. 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.