Sunrise Thread AI Specific Terms

1. Sunrise Thread AI is an ambient listening software module that utilizes artificial intelligence ("AI") for clinical note documentation (the "Software"). The intended use of the Software is to capture a conversation in the exam room between the patient and health care provider, summarize the conversation in the clinical note and extract the unstructured data to create structured clinical note documentation (the "Output"). If properly used, the intended benefits are for the Software to help facilitate more natural patient–health care provider interactions, decrease documentation burdens for health care providers, and enhance the accuracy and consistency of clinical note authoring.

2. Altera reserves the right to modify or update these terms at any time without prior notice. Any changes will be effective immediately upon posting the updated terms on Altera's website: www.alterahealth.com/legal. Client's continued use of the Software following the posting of any changes constitutes your acceptance of the updated terms. It is Client's responsibility to review these terms regularly to ensure Client is aware of any changes.

3. AI is emergent technology, and third-party vendors may discontinue providing or modify the services at any time. Accordingly, Altera may, at its discretion, replace third party software or services providers use to provide the Software at any time. These terms will be updated to reflect the current third-party software or services powering the Software. Altera also reserves the right to suspend the Software to resolve confidentiality concerns, security concerns, a threat to the functionality of the Software, patient safety or other exigent issues. Altera will provide notice of such suspension as soon as practicable and restore the Software upon resolution.

4. The Software is powered by third party software or services licensed from Soniox, Inc. and Microsoft Corporation. Third party software may have separate software specific terms and conditions that apply to its use and are available at www.alterahealth.com/legal, which may be modified from time to time. Such modifications will become effective upon posting to the foregoing link. Altera makes no representation or warranty with respect to any third-party software or services or any third-party equipment, including but not limited to, the Soniox, Inc. or Microsoft software. Client agrees with any applicable third-party terms by its use of the Software.

5. This Software will transmit Protected Health Information ("PHI") to Microsoft, and such PHI will be subject to Microsoft's Business Associate Agreement ("BAA"), which may contain different risk allocation provisions than Client's BAA with Altera. By using the Software, Client hereby agrees to Microsoft's BAA with respect to any PHI processed by the Software. A copy of Microsoft's BAA is available at the end of these terms for Client's convenience, but the BAA may be updated from time to time, so the most current version will be available on Microsoft's website.

6. The Software uses AI and machine learning models that generate predictions based on patterns in data. Output generated by a machine learning model is probabilistic. The Software is not responsible for making any decisions and is simply applying computer logic to conversations. THE OUTPUT PRODUCED BY THE SOFTWARE IS BASED IN PART ON CLIENT DATA AND OTHER DATA

SUPPLIED BY THIRD PARTIES, HEALTHCARE PROVIDERS, PATIENTS, AND/OR CLIENT. THE CLIENT MUST REVIEW AND CONFIRM THAT ALL OUTPUT IS TRUE, ACCURATE AND CORRECT. CLIENT IS SOLELY RESPONSIBLE FOR REVIEWING, IDENTIFYING, AND CORRECTING ERRORS AND INACCURACIES AND APPROVING ALL OUTPUT PREPARED USING THE SOFTWARE BEFORE USING AND/OR RELYING ON THE OUTPUT FOR ANY PURPOSE, AND ALTERA HAS NO LIABILITY OR RESPONSIBILITY WHATSOEVER FOR THE ACCURACY, COMPLETENESS, OR CONTENT OF ANY OUTPUT. CLIENT SHALL REPORT ISSUES RELATED TO THE OUTPUT TO ALTERA.

7. Client hereby represents and warrants that Client shall comply with all applicable laws that concern this Agreement or the subject matter hereof, including but not limited to, by providing Notices (defined herein below) and when utilizing the Software. Client hereby represents and warrants that Client has all rights necessary, including Required Authorizations (defined herein below), to grant and hereby grants Altera the right to access, use, and disclose the Client Data and Output only for the purposes of or in connection with: (a) providing the Software; (b) creating De-Identified Data; and (c) for other purposes permitted by law. “Client Data” means any data, media, documents, content, and other materials that are provided to Altera by or on behalf of Client pursuant to this Agreement, including recordings and transcriptions and other data entered into the Software as a result of Client’s use of the Software. “De-Identified Data” means Client Data that has been de-identified in accordance with HIPAA’s requirements for de-identification set forth at 45 CFR 164.514(b). Client hereby grants Altera the right to use and disclose De-Identified Data, during and after the Agreement Term, for any purpose unless prohibited by applicable law, including but not limited to, the right to use and disclose De-Identified Data to analyze, test, develop, maintain, refine, train, tune, improve, enhance, optimize, automate, and expand the insights, processes, methods, and tools relating to the Software and any other Altera products and services. Client is solely responsible for ensuring the accuracy and completeness of the Client Data, and Altera shall not be liable for damage or deficiency with respect to Client Data.

8. Prior to Client providing any Client Data to Altera or otherwise using the Software, Client shall be solely responsible for providing Notices to, and obtaining any Required Authorizations from, any patient, provider, and other individual whose Personal Data is included in any recording, transcription, or who is present during the Software’s use and provides such Personal Data during that recording. “Required Authorization” means, as and to the extent required by applicable law, any consent (a) to collect, capture, make, and/or store recordings and transcriptions relating to individuals, including, but not limited to, the consent to use AI to do any of the foregoing; and/or (b) to use and disclose a recording, transcription, an individual’s PHI, or other Personal Data for purposes described in this Agreement, including, but not limited to, the consent to use any of the foregoing with AI. “Notice” means notices and/or disclosures required by applicable law to be presented or otherwise made to individuals in relation to the use or disclosure of their Personal Data and/or the use of AI, including, but not limited to, employee privacy notices, privacy policies, Notices of Privacy Practices, and disclosures required by laws regulating the use of AI (e.g., the Utah Artificial Policy Act). “Personal Data” means all data defined as personally identifiable information, personal information, or personal data under applicable law and includes PHI. All Required Authorizations will be maintained by Client

for a period as required by applicable law, including HIPAA, and provided to Altera promptly upon written request.

9. DISCLAIMER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE IS EXPERIMENTAL IN NATURE AND IS BEING PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS AND MAY CONTAIN SIGNIFICANT ERRORS, DATA LOSS, OMISSIONS, AND OTHER PROBLEMS. ALTERA DISCLAIMS ALL WARRANTIES, RESPONSIBILITIES, AND LIABILITIES WITH RESPECT TO THE FOREGOING, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. NOTWITHSTANDING ANYTHING ELSE, (A) ALTERA DOES NOT COVENANT, REPRESENT, OR WARRANT THAT THE SOFTWARE WILL MEET CLIENT'S REQUIREMENTS OR YIELD ANY PARTICULAR BUSINESS OR FINANCIAL RESULT, OR THAT OPERATION OF THE SERVICES OR THE SOFTWARE WILL BE SECURE, ERROR FREE, VIRUS FREE OR UNINTERRUPTED, THAT ANY DATA WILL BE ACCURATE OR RELIABLE, THAT ANY SOFTWARE OR DATA WILL NOT BE LOST OR CORRUPTED, OR THAT IT WILL BE ABLE TO RECTIFY/REMEDY ANY ERRORS OR DEFECTS, (B) ALTERA BEARS NO RESPONSIBILITY OR LIABILITY AS TO THE QUALITY AND PERFORMANCE OF THE SERVICES OR SOFTWARE, (C) ALTERA IS A TECHNOLOGY COMPANY AND DOES NOT PROVIDE MEDICAL ADVICE OR HEALTHCARE SERVICES, AND (D) THE SOFTWARE AND OUTPUT ARE NOT INTENDED TO REPLACE THE PROFESSIONAL SKILLS, JUDGMENT, OR ADVICE OF A HEALTHCARE PROVIDER AND THE OUTPUT SHOULD BE USED BY COMPETENT PROFESSIONALS IN MAKING HEALTHCARE DECISIONS. ALTERA WILL NOT UNDER ANY CIRCUMSTANCE BE RESPONSIBLE OR LIABLE FOR ANY PRIVACY, CONFIDENTIALITY, SECURITY, AND/OR AVAILABILITY ISSUE AND/OR ANY LOSS OF ANY DATA RELATED TO OR ARISING FROM CLIENT'S COMPUTER SYSTEMS, CLIENT'S SOFTWARE, OR THE CLIENT'S EQUIPMENT THAT IS UTILIZED DURING THE USE OF THE SOFTWARE.

Microsoft’s HIPAA Business Associate Agreement
Last Updated May 2025

HIPAA Business Associate Agreement

If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Data, FastTrack Data, or Professional Services Data, this HIPAA Business Associate Agreement ("BAA") is incorporated upon execution of an agreement ("Agreement") that incorporates the Microsoft Products and Services Data Protection Addendum. 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 Microsoft by or on behalf of Customer for Microsoft'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); and (2) Dynamics 365 Core Services and Microsoft Power Platform Core Services; that are provided to Customer by Microsoft in connection with Customer's Microsoft Online Services subscription, excluding services that are performed using third-party software or software that is not hosted by Microsoft.

"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.

"Microsoft BAA-Scope Services", for this BAA only, means the Core Online Services as defined in the Product Terms incorporated into the Agreement; Azure Health Bot; Windows 365; and any additional Azure online services and U.S. Government online services listed as in scope for this BAA on the Microsoft Trust Center at https://docs.microsoft.com/en-us/compliance/regulatory/offering-hipaa-hitech (or successor site); excluding Previews.

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

"Professional Services" has the meaning provided in the Microsoft Products and Services Data Protection Addendum. For clarity, the Supplemental Professional Services in scope for this BAA are the FastTrack Services.

"Professional Services Data" means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from an Online Service) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services.

"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 (a) through the use of the Microsoft BAA-Scope Services, (b) for Microsoft's performance of the FastTrack Services, or (c) through Microsoft's provision of Professional 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.** Except as otherwise limited in this BAA, 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 or as listed as an exception to the DPA in the Privacy and Security Terms section of the Product Terms.

b. **Management, Administration, and Legal Responsibilities.** Except as otherwise limited in this BAA, 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 BAA 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 BAA. Microsoft BAA-Scope Services, FastTrack Services, and Professional Services shall not use Protected Health Information for any advertising, Marketing or similar 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 Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; 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 BAA 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 seventy-two (72) hours after Microsoft's 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 BAA 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 BAA.

(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 Processed Data" within the Microsoft Products and Services Data Protection Addendum.

(vi) Access. The parties acknowledge and agree that Microsoft does not maintain Protected Health Information in a Designated Record Set for Customer. In the event that there is a change in the Microsoft BAA-Scope Services, FastTrack Services, or Professional Services that Microsoft provides to Customer such that Microsoft commences maintaining Protected Health Information in a Designated Record Set, 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. Subject to Section 3a(vi) above, 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 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 thirty (30) 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 BAA will be provided as set forth in the Agreement.

(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 outside of Professional Services, or, for Professional Services, within the subject or body of a support case management or support ticket; 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, FastTrack Data, or Professional Services Data once it is sent to or from Customer outside Microsoft BAA-Scope Services, FastTrack Services, or Professional Services over the public Internet, or if Customer fails to follow applicable instructions regarding physical media transported by a common carrier.

2) During use of Microsoft BAA-Scope Services or in an engagement with Microsoft to obtain Professional Services or FastTrack Services, implement privacy and security safeguards in the systems, applications, and software that Customer controls, configures, and uploads.

4. Applicability of BAA.

This BAA is applicable to Microsoft BAA-Scope Services, FastTrack Services, and Professional Services. Microsoft may, from time to time, (a) include additional Microsoft online services on the Microsoft Trust Center and/or in the Microsoft Products and Services Data Protection Addendum incorporated into the Agreement or additional FastTrack Services on the FastTrack Center BAA site, and (b) update the definition of Microsoft BAA-Scope Services, FastTrack Services, and Professional Services in this BAA, 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 Microsoft 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 5.b., 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, 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 Agreement. If it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this BAA, then Microsoft 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. **Amendments; 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 Microsoft 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 Microsoft an agent of Customer.