TWEHR Note+ and Note+ Ambient Listening Specific Terms

1. TWEHR Note+ is an ambient listening software module that utilizes artificial intelligence (AI) for clinical note documentation (collectively, 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 Microsoft Corporation and Google LLC ("Google"). 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 Microsoft or Google 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 Google Gemini, and such PHI will be subject to Google's Business Associate Addendum ("BAA"), which may contain different risk allocation provisions than Client's BAA with Altera. By using the Software, Client hereby agrees to Google's BAA with respect to any PHI processed by the Software. Google's BAA is available at: https://cloud.google.com/terms/hipaa-baa?sjid=98750060048749706-NA and a copy 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 at the link above.

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.

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.

Google Cloud Platform HIPAA Business Associate Addendum

Available at: ***https://cloud.google.com/terms/hipaa-baa?sjid=987500600487497706-NA***

This HIPAA Business Associate Addendum ("BAA") is entered into between Google LLC ("Google") and the customer agreeing to the terms below ("Customer"), and supplements, amends and is incorporated into the Services Agreement(s) (defined below) solely with respect to Covered Services (defined below). This BAA will be effective when Customer clicks to accept this BAA (the "BAA Effective Date").

Customer must have an existing Services Agreement in place for this BAA to be valid and effective. Together with the Services Agreement, this BAA will govern each party's respective obligations regarding Protected Health Information (defined below).

You represent and warrant that (i) you have the full legal authority to bind Customer to this BAA, (ii) you have read and understand this BAA, and (iii) you agree, on behalf of Customer, to the terms of this BAA. If you do not have legal authority to bind Customer, or do not agree to these terms, please do not click to accept the terms of this BAA.

1. Definitions

Any capitalized terms used but not otherwise defined in this BAA will have the meaning given to them in either (i) HIPAA and the HITECH Act or (ii) the Services Agreement(s).

"Business Associate" has the definition given to it under HIPAA at 45 CFR § 160.103.
"Breach" has the definition given to it under HIPAA at 45 CFR § 164.402. A Breach will not include an acquisition, access, use, or disclosure of PHI with respect to which Google has determined in accordance with 45 C.F.R. § 164.402 that there is a low probability that the PHI has been compromised.
"Breach Notification Rule" means the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.
"Covered Entity" has the definition given to it under HIPAA at 45 CFR § 160.103.
"Covered Services" means the Google products and services specifically identified at https://cloud.google.com/security/compliance/hipaa/ and, as applicable at https://cloud.google.com/terms/secops/hipaacoveredservices, as being covered by the Google Cloud Platform BAA.
"Designated Record Set" has the definition given to it under HIPAA at 45 CFR § 164.501.
"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended, including the Privacy Rule, the Breach Notification Rule and the Security Rule, and amendments to HIPAA made by the HITECH Act.
"HIPAA Implementation Guide" means the informational guide that Google makes available describing how the Covered Services may be configured by Customer in connection with Customer's HIPAA compliance efforts. The HIPAA Implementation Guide for the Covered Services is available for review at the following URL: https://cloud.google.com/security/compliance/hipaa/ and, as applicable at https://cloud.google.com/terms/secops/hipaacoveredservices.

“HITECH Act” means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.
“Privacy Rule” means the HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164.
“Protected Health Information” or “PHI” has the definition given to it under HIPAA at 45 CFR § 160.103, and for purposes of this BAA is limited to PHI within Customer Data to which Google has access through the Covered Services in connection with Customer’s permitted use of Covered Services.
“Required by Law” has the definition given to it under HIPAA at 45 CFR § 160.103.
“Security Incident” has the definition given to it under HIPAA at 45 CFR § 164.304.
“Services Agreement(s)” means the written agreement(s) entered into between Google and Customer for provision of the Covered Services, which agreement(s) may be in the form of online terms of service.
“Security Rule” means the HIPAA Security Rule, 45 CFR parts 160 and 164, subparts A and C.

2. Applicability of this BAA.
This BAA applies to the extent Customer is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI via a Covered Service and to the extent Google, as a result, is acting as a Business Associate or Subcontractor of Customer under HIPAA. This BAA does not apply to any Google product, service, or feature that is not a Covered Service. This BAA does not apply to PHI that Customer creates, receives, maintains, or transmits outside of the Covered Services (including Customer’s use of its offline or on-premise storage tools or third-party applications).

3. Permitted and Required Use and Disclosure of Protected Health Information.
(a) Performance of the Agreement. Except as otherwise limited by this BAA, Google may only use and disclose PHI for or on behalf of Customer as permitted or required by the Services Agreements, this BAA, or as Required by Law.

(b) Management, Administration, and Legal Responsibilities. Google may use and disclose PHI for the proper management and administration of Google business and / or to carry out Google’s legal responsibilities, provided that any disclosure of PHI by Google for such purposes may only occur if: (i) Required by Law; or (ii) Google takes appropriate measures to ensure that any person to whom PHI will be disclosed is bound by written obligations that provide the same material level of protection for PHI as this BAA.

4. Google Responsibilities with Respect to Protected Health Information.
When Google is acting as a Business Associate under this BAA, Google will fulfill the following obligations:

(a) Appropriate Safeguards. Google will use appropriate safeguards designed to prevent unauthorized use or disclosure of PHI, and as otherwise required under HIPAA, with respect to the Covered Services. Google will implement all requirements of the HIPAA Security Rule with regard to electronic PHI.

(b) Reporting and Related Obligations.

(i) Security Incident and Breach Reporting. Google will promptly notify Customer of (i) any Security Incident of which Google becomes aware, subject to Section 4(b)(iii); and (ii) any Breach that Google discovers, including Breaches of unsecured PHI in accordance with 45 CFR § 164.410 of the Breach Notification Rule, provided that any notice for Breach will be made promptly and without unreasonable delay. Notifications made under this section will describe, to the extent possible, details of a Breach, including steps taken to mitigate the potential risks and steps Google recommends Customer take to address the Breach.

(ii) Notification. Google will send any applicable notifications to the notification email address provided by Customer in the Agreement or via direct communication with Customer.

(iii) Unsuccessful Attempts. Notwithstanding Section 4(b)(i), this Section 4(b)(iii) will be deemed as notice to Customer that Google periodically receives unsuccessful attempts (including without limitation pings, unsuccessful log-on attempts, denial of service attacks, port scans and attempts) for unauthorized access, use, disclosure, modification, or destruction of information, or interference with the general operation of Google's systems and the Covered Services. Customer acknowledges and agrees that even if such events constitute a Security Incident, Google will not be required to provide any notice under this BAA regarding such unsuccessful attempts other than this Section 4(b)(iii).

(c) Subcontractors. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Google will take appropriate measures to ensure that any Subcontractors used by Google to perform its obligations under the Agreement that require access to PHI on behalf of Google are bound by written obligations that provide the same material level of protection for PHI as this BAA. To the extent Google uses Subcontractors in its performance of obligations hereunder, Google will remain responsible for their performance as if performed by Google.

(d) Access and Amendment. Customer acknowledges and agrees that Customer is solely responsible for the form and content of PHI maintained by Customer within the Covered Services, including whether Customer maintains such PHI in a Designated Record Set within the Covered Services. The parties acknowledge and agree that Google does not maintain PHI in a Designated Record Set for Customer.Google will make available PHI for amendments (and incorporate any amendments, if required) and accountings in accordance with 45 CFR § 164.526 and 45 CFR § 164.528 of the Privacy Rule. Google will provide Customer with access to Customer's PHI via the Covered Services so that Customer may fulfill its obligations under HIPAA with respect to Individuals' rights of access and amendment, but will have no other obligations to Customer or any Individual with respect to the rights afforded to Individuals by HIPAA with respect to Designated Record Sets, including rights of access or amendment of PHI. Customer is responsible for managing its use of the Covered Services to appropriately respond to such individual requests.

(e) Accounting of Disclosures. When requested by Customer, Google will document disclosures of PHI by Google and provide an accounting of such disclosures to Customer as and to the extent required of a Business Associate under HIPAA and in accordance with the requirements applicable to a Business Associate under HIPAA. Because Google is unable to readily identify which Individuals are identified or what types of PHI are included in PHI Customer or any of Customer's End User submit to the Covered Services under Customer's Account, Customer will be solely responsible for identifying any Individuals who may have been included in PHI that Google has disclosed and for providing a description of the PHI disclosed.

(f) Secretary's Access to Records. Google will make its internal practices, books, and records concerning the use and disclosure of PHI received from Customer, or created or received by Google on behalf of Customer, available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for the purpose of the Secretary determining compliance with this BAA to the extent required by law, and subject to all applicable legal privileges. The Legal Process section of the General Terms of the Agreement will apply to Google's response to such requests by the Secretary.

(g) Return/Destruction of Information. On termination of the Agreement, Google will return or destroy all PHI received from Customer, or created or received by Google on behalf of Customer; provided, however, that if such return or destruction is not feasible, Google will extend the protections of this BAA to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

(h) Performance of a Covered Entity's Obligations. To the extent Google agrees in writing to carry out a Covered Entity's obligation under the Privacy Rule, Google shall comply with the requirements applicable to such obligation.

5. Customer Responsibilities with Respect to Protected Health Information.
(a) Impermissible Requests. Customer will not request that Google or the Covered Services use or disclose PHI in any manner that would not be permissible under HIPAA if done by Customer (if Customer is a Covered Entity) or by the Covered Entity to which Customer is a Business Associate (unless expressly permitted under HIPAA for a Business Associate).

(b) Use of Service Controls. For Customer's End Users that use the Covered Services in connection with PHI, Customer will use controls available within the Services, including those detailed in the HIPAA Implementation Guide, to ensure its use of PHI is limited to the Covered Services. Customer acknowledges and agrees that the HIPAA Implementation Guide is provided by Google solely as an optional, informational guide with respect to Customer's configuration options, and that Customer is solely responsible for ensuring that its and its End Users' use of the Covered Services complies with HIPAA and the HITECH Act.

(c) Appropriate Safeguards. Customer will use appropriate safeguards designed to prevent unauthorized use or disclosure of PHI, and as otherwise required under HIPAA, with respect to the Covered Services

6. Term and Termination of this Business Associate Addendum.
(a) Term. The term ("Term") of this BAA will begin on the BAA Effective Date and end on the earlier of (i) termination in accordance with Section 6, or (ii) the expiration or termination of all Services Agreements under which Customer has access to a Covered Service.

(b) Termination for Breach. If either party materially breaches this BAA, the non-breaching party may terminate this BAA on 10 days' written notice ("Termination Notice Period") to the breaching party unless the breach is cured within the Termination Notice Period. If a cure under this Section 6(b) is not reasonably possible, the non-breaching party may immediately terminate this BAA, or if neither termination nor cure is reasonably possible under this Section 6(b), the non-breaching party may report the violation to the Secretary, subject to all applicable legal privileges.

(c) Use of the Services after Termination. If this BAA is terminated earlier than the Services Agreements, Customer may continue to use the Services in accordance with the Services Agreements on the condition that, before the end of the Termination Notice Period, Customer deletes any PHI it maintains in the Covered Services and immediately upon termination ceases to further create, receive, maintain, or transmit such PHI to Google.

7. Miscellaneous.
(a) Survival. Sections 4(g) (Return/Destruction of Information) and 7 (Miscellaneous) will survive termination or expiration of this BAA.

(b) Effects of BAA. To the extent this BAA conflicts with the remainder of the Services Agreement(s), this BAA will govern. This BAA is subject to the "Governing Law" section in the Services Agreement(s). Except as expressly modified or amended under this BAA, the terms of the Services Agreement(s) remain in full force and effect.

(c) No Third Party Beneficiaries. This BAA does not give any person other than Customer and Google, and their respective successors or assigns, any rights or obligations under this BAA.