BUSINESS ASSOCIATE AGREEMENT

Version 1.0 · Effective August 1, 2026 · Pippa LLC

This Business Associate Agreement (this "Agreement") supplements and is made a part of the Services Agreement (as defined below) by and between the entity identified as the customer in the Services Agreement ("Organization") and Pippa LLC, a limited liability company ("Pippa" or "Business Associate"). This Agreement is effective as of the effective date of the Services Agreement, or as of the date of the last signature below if executed separately (the "Effective Date").

WHEREAS, Pippa provides Organization with software and related services for eating-disorder and nutrition care, which may include photograph-based meal logging, meal plans and grocery lists, structured post-meal and daily check-ins, mood entries, clinician-configured questionnaires, in-application messaging between patients and their care team, automated safety flagging, and a clinician dashboard through which Organization's workforce reviews patient information (collectively, the "Services");

WHEREAS, in performing the Services, Pippa creates, receives, maintains, or transmits Protected Health Information on behalf of Organization, and therefore meets the definition of a Business Associate set forth at 45 C.F.R. § 160.103;

WHEREAS, this Agreement defines the rights and responsibilities of each party with respect to Protected Health Information under the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and the regulations promulgated thereunder, as each may be amended from time to time (collectively, the "HIPAA Regulations");

WHEREAS, this Agreement is intended to satisfy the applicable requirements of 45 C.F.R. §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e);

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. Definitions

(a) General. Capitalized terms used but not otherwise defined in this Agreement have the meanings given to them by the HIPAA Regulations.

(b) Specific. For purposes of this Agreement:

(i) "Breach" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.

(ii) "Business Associate" has the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and in reference to a party to this Agreement means Pippa.

(iii) "Covered Entity" has the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to a party to this Agreement means Organization.

(iv) "Designated Record Set" has the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.

(v) "Electronic Protected Health Information" or "Electronic PHI" has the same meaning as the term "electronic protected health information" at 45 C.F.R. § 160.103, limited to the information Pippa creates, receives, maintains, or transmits from or on behalf of Organization.

(vi) "Individual" has the same meaning as the term "individual" at 45 C.F.R. § 160.103 and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g), including a parent or legal guardian acting on behalf of a minor patient.

(vii) "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

(viii) "Protected Health Information" or "PHI" means individually identifiable health information, as that term is defined at 45 C.F.R. § 160.103, limited to the information created or received by Pippa from or on behalf of Organization in connection with the Services.

(ix) "Required By Law" has the same meaning as the term "required by law" at 45 C.F.R. § 164.103.

(x) "Secretary" means the Secretary of the U.S. Department of Health and Human Services or the Secretary's designee.

(xi) "Security Incident" has the same meaning as the term "security incident" at 45 C.F.R. § 164.304.

(xii) "Security Rule" means the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

(xiii) "Services Agreement" means any present or future agreement, written or electronic, between Organization and Pippa under which Pippa provides the Services to Organization and which involves the creation, receipt, maintenance, transmission, access, use, or disclosure of PHI.

(xiv) "Subcontractor" has the same meaning as the term "subcontractor" at 45 C.F.R. § 160.103.

(xv) "Unsecured Protected Health Information" or "Unsecured PHI" has the same meaning as the term "unsecured protected health information" at 45 C.F.R. § 164.402.

2. Obligations of Pippa

(a) Use and Disclosure. Pippa will not use or disclose PHI other than as permitted or required by the Services Agreement, this Agreement, or as Required By Law. Pippa will not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Organization.

(b) Safeguards. Pippa will use appropriate administrative, physical, and technical safeguards, and will comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Services Agreement or this Agreement. Without limiting the foregoing, and as of the Effective Date, Pippa maintains the following controls:

(i) PHI is encrypted in transit and at rest and is stored in access-controlled cloud infrastructure located in the United States.

(ii) Every access to patient data by a member of Organization's workforce through the clinician dashboard is written to an append-only audit log available to Organization.

(iii) Access to production systems by Pippa personnel is limited to those with a business need, is granted on a least-privilege basis, and is logged.

(iv) Meal photographs are re-encoded on the patient's device before upload, which removes embedded metadata including location data. Pippa performs no facial recognition or other biometric processing on any image.

(v) Pippa maintains a written security program, workforce security training, and an incident response process, and will make a summary of its security posture available to Organization on reasonable request.

(c) Prohibited Uses. In addition to the restrictions imposed by the HIPAA Regulations, Pippa will not: (i) sell PHI or receive remuneration in exchange for PHI; (ii) use or disclose PHI for marketing or advertising, or share PHI with advertising networks, data brokers, or third-party analytics providers; or (iii) use PHI, or permit any Subcontractor to use PHI, to train, fine-tune, or otherwise improve any machine learning or artificial intelligence model. Pippa's agreements with its artificial-intelligence Subcontractors prohibit the use of Organization's content for model training.

(d) Reporting. Pippa will report to Organization any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, any Security Incident with respect to Electronic PHI, and any Breach of Unsecured PHI, in accordance with 45 C.F.R. § 164.410.

(i) Pippa will notify Organization of a Breach of Unsecured PHI without unreasonable delay and in no event later than ten (10) business days after Discovery, and will supplement that notice as further information becomes available.

(ii) The notice will include, to the extent then known, the identification of each Individual whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired, used, or disclosed; a description of what happened; the date of the Breach and the date of Discovery; the types of information involved; and the steps Pippa is taking to investigate, mitigate, and prevent recurrence.

(iii) The parties acknowledge that unsuccessful Security Incidents that do not result in unauthorized access to, or use, disclosure, modification, or destruction of, Electronic PHI — such as unsuccessful log-in attempts, pings, port scans, and denials of service — occur frequently, and this paragraph constitutes notice of them. No additional report of such incidents is required.

(iv) Organization is responsible for any notification to Individuals, the Secretary, or the media required by 45 C.F.R. §§ 164.404, 164.406, and 164.408. Pippa will cooperate with and support Organization in preparing and delivering those notifications at no additional charge.

(e) Subcontractors. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), Pippa will require each Subcontractor that creates, receives, maintains, or transmits PHI on Pippa's behalf to agree in writing to restrictions and conditions at least as protective as those that apply to Pippa under this Agreement. Pippa remains responsible to Organization for its Subcontractors' performance. As of the Effective Date, Pippa's Subcontractors that may process PHI are Amazon Web Services (database, identity, and transactional email), Cloudflare (application hosting and meal-photograph storage), OpenAI (chat responses, meal-photograph food and portion estimates, and safety moderation), Apple (push notifications, platform sign-in), and Google (push notifications on Android, platform sign-in). Pippa maintains a current list of Subcontractors and will make it available to Organization on request.

(f) Compliance with Organization's Obligations. To the extent Pippa is to carry out one or more of Organization's obligations under Subpart E of 45 C.F.R. Part 164, Pippa will comply with the requirements of Subpart E that apply to Organization in the performance of those obligations.

(g) Access by Individuals. Pippa will make PHI it maintains in a Designated Record Set available to Organization, or as directed by Organization to an Individual, in the time and manner reasonably necessary for Organization to satisfy 45 C.F.R. § 164.524, and in any event within ten (10) business days of Organization's request. Where the Services make PHI directly available to Organization through the clinician dashboard or an export function, Organization's use of that function satisfies this paragraph. Pippa is not obligated to respond to a request made directly to Pippa by an Individual and will instead refer the Individual to Organization, except where the Individual is exercising rights with respect to Pippa's own consumer-facing service.

(h) Amendment of PHI. Pippa will make PHI it maintains in a Designated Record Set available for amendment, and will incorporate any amendment Organization directs, as necessary for Organization to satisfy 45 C.F.R. § 164.526, within ten (10) business days of Organization's request.

(i) Accounting of Disclosures. Pippa will document disclosures of PHI and information related to those disclosures as would be required for Organization to respond to a request for an accounting of disclosures under 45 C.F.R. § 164.528, and will provide that documentation to Organization within ten (10) business days of request.

(j) Restrictions and Confidential Communications. Pippa will comply with any restriction on the use or disclosure of PHI, and any request for confidential communications, that Organization has agreed to under 45 C.F.R. § 164.522 and communicated to Pippa in writing, to the extent the restriction is technically supported by the Services.

(k) Access to Books and Records. Pippa will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary, in the time and manner designated by the Secretary, for purposes of determining Organization's compliance with the HIPAA Regulations. Pippa will not charge Organization for time spent complying with this paragraph. Pippa will notify Organization of any such request unless prohibited from doing so.

(l) Mitigation. Pippa will mitigate, to the extent practicable, any harmful effect known to Pippa of a use or disclosure of PHI by Pippa in violation of this Agreement.

(m) Workforce. Pippa will train members of its workforce who have access to PHI on their obligations under this Agreement and the HIPAA Regulations, and will apply appropriate sanctions against workforce members who fail to comply.

3. Permitted Uses and Disclosures by Pippa

(a) Performance of the Services. Except as otherwise limited by this Agreement, Pippa may use and disclose PHI to perform the functions, activities, and services described in the Services Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Organization.

(b) Minimum Necessary. Pippa will limit its use, access, and disclosure of PHI to the minimum amount reasonably necessary to accomplish the intended purpose, consistent with 45 C.F.R. § 164.502(b) and any guidance issued by the Secretary.

(c) Management and Administration. Except as otherwise limited by this Agreement, Pippa may use PHI for the proper management and administration of Pippa and to carry out Pippa's legal responsibilities.

(d) Disclosure for Management and Administration. Except as otherwise limited by this Agreement, Pippa may disclose PHI for the proper management and administration of Pippa or to carry out Pippa's legal responsibilities, provided that (i) the disclosure is Required By Law, or (ii) Pippa obtains reasonable assurances from the person to whom the PHI 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, and that the person will notify Pippa of any instance of which it becomes aware in which the confidentiality of the information has been breached.

(e) Data Aggregation. Pippa may use and disclose PHI to provide data aggregation services relating to the health care operations of Organization, as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

(f) Violations of Law. Pippa may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

(g) De-identified Information. Pippa may de-identify PHI in accordance with 45 C.F.R. § 164.514(a)–(c) and may use and disclose the resulting de-identified information for its business purposes, including improving the Services and providing reporting to Organization. Pippa will not attempt to re-identify de-identified information, will not sell or license de-identified information derived from Organization's PHI, and will not use it to train, fine-tune, or improve any artificial intelligence model.

(h) Safety Escalation. The Services include automated flagging of patient content that may indicate a crisis. Where a patient has an active data-sharing relationship with Organization, Pippa will disclose the flag and its context to Organization as a disclosure for treatment purposes on Organization's behalf. Where no such relationship exists, Pippa will present crisis resources directly to the patient and may use or disclose the information to the extent permitted by 45 C.F.R. § 164.512(j). Organization acknowledges that Pippa does not monitor the Services on a continuous basis and that clinical response is Organization's responsibility.

4. Obligations of Organization

(a) Notice of Privacy Practices. Organization will notify Pippa of any limitation in Organization's notice of privacy practices under 45 C.F.R. § 164.520 to the extent the limitation may affect Pippa's use or disclosure of PHI.

(b) Changes in Permission. Organization will notify Pippa of any change in, or revocation of, an Individual's permission to use or disclose PHI to the extent the change may affect Pippa's use or disclosure of PHI.

(c) Restrictions. Organization will notify Pippa of any restriction on the use or disclosure of PHI that Organization has agreed to under 45 C.F.R. § 164.522 to the extent the restriction may affect Pippa's use or disclosure of PHI.

(d) Permissible Requests. Organization will not request Pippa to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Organization, except as permitted by Section 3(c) through 3(g) of this Agreement.

(e) Consent and Authorization. Organization is responsible for obtaining and maintaining any consent, authorization, or assent legally required for a patient to use the Services and for Organization's workforce to access that patient's PHI, including consent from a parent or legal guardian where the patient is a minor and the law of the applicable jurisdiction requires it. Organization represents that each patient it enrolls is a patient of Organization and that Organization has satisfied this obligation.

(f) Workforce Access. Organization is responsible for determining which members of its workforce receive access to the clinician dashboard, for the accuracy of the accounts it creates, and for promptly deactivating accounts when a workforce member's access is no longer appropriate. Organization will safeguard credentials and enrollment codes issued to it.

5. Term and Termination

(a) Term. This Agreement takes effect on the Effective Date and continues for the term of the Services Agreement and thereafter until all PHI is returned to Organization or destroyed in accordance with Section 5(c).

(b) Termination for Cause. A material breach of this Agreement is a material breach of the Services Agreement. If either party knows of a pattern of activity or practice of the other party that constitutes a material breach of the other party's obligations under this Agreement, the non-breaching party will provide written notice and a reasonable opportunity to cure, not to exceed thirty (30) days, and may terminate the Services Agreement if the breach is not cured within that period or if cure is not feasible.

(c) Effect of Termination. On termination of the Services Agreement for any reason, Pippa will, at Organization's election, return to Organization or destroy all PHI in its possession, and will require its Subcontractors to do the same. Pippa's standard practice is permanent erasure of patient data from its production systems within thirty (30) days of the termination or deletion request, with backup copies aging out on Pippa's ordinary rotation schedule. Pippa may retain the following, keyed to internal identifiers rather than patient names or contact information, for approximately six (6) years or such other period as law requires: records of consent grants and revocations, records of deletion requests, and clinician-access audit logs. Where return or destruction of PHI is infeasible, Pippa will notify Organization of the conditions that make it infeasible, will extend the protections of this Agreement to that PHI, and will limit further use and disclosure to the purposes that make return or destruction infeasible, for so long as Pippa maintains it. Pippa will not charge Organization for return, destruction, or continued protection of PHI under this paragraph.

6. General

(a) Amendment. The parties will take such action as is reasonably necessary to amend this Agreement from time to time so that each party may comply with the HIPAA Regulations as they may be amended. If a required amendment would materially increase Pippa's cost of providing the Services, Pippa may terminate the Services Agreement on thirty (30) days' written notice, with a pro-rata refund of any prepaid, unused fees.

(b) Survival. The rights and obligations of the parties under Sections 2, 3, 5(c), and 6 survive termination of this Agreement and the Services Agreement.

(c) Interpretation. Any ambiguity in this Agreement will be resolved to permit Organization and Pippa to comply with the HIPAA Regulations. References to a section of the HIPAA Regulations mean that section as in effect or as amended, and include any successor provision.

(d) No Third-Party Beneficiaries. Nothing in this Agreement is intended to confer, nor will anything herein confer, any rights or remedies on any person other than Organization, Pippa, and their respective successors and permitted assigns.

(e) Independent Contractors. Nothing in this Agreement creates a partnership, joint venture, agency, or employment relationship between the parties. Pippa is not a health care provider and does not practice medicine, dietetics,

psychotherapy, or any other licensed profession, and the Services are not a substitute for clinical judgment.

(f) Conflict. The terms of this Agreement are incorporated into the Services Agreement. In the event of a conflict between this Agreement and the Services Agreement with respect to PHI, this Agreement controls.

(g) Governing Law. This Agreement is governed by and construed in accordance with the law that governs the Services Agreement, exclusive of its conflict-of-law rules, and in all cases subject to applicable federal law.

(h) Entire Agreement. The Services Agreement together with this Agreement constitutes the entire agreement between the parties with respect to the subject matter of this Agreement, and this Agreement supersedes and replaces any prior business associate agreement or addendum between the parties.

(i) Counterparts and Signatures. This Agreement may be executed in counterparts, each of which is an original and all of which together constitute one instrument. Signatures delivered by PDF, facsimile, or electronic signature are deemed original signatures.

(j) Amendment and Waiver. No amendment or modification of this Agreement, and no waiver of any provision, is effective except in a writing signed by both parties. A waiver with respect to one event is not a continuing waiver and does not bar the exercise of any right or remedy as to subsequent events.

(k) Notices. Notices under this Agreement must be in writing and are effective when delivered to the address stated in the Services Agreement or, for notices to Pippa, when sent to pippa.app.general@gmail.com with a subject line identifying this Agreement. Breach notifications under Section 2(d) may be given by email to Organization's designated privacy contact.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

ORGANIZATION

Entity name

Signature

Printed name

Title

Date

PIPPA LLC

Signature

Printed name

Title

Date