

MEDCORE ANALYTICS INC.

200 CentrePort Drive, Suite 350 | Greensboro, NC 27409 | (336) 555-0217

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into as of February 10, 2026 (the "Effective Date"), by and between:

MEDCORE ANALYTICS INC., a North Carolina corporation ("Controller"), with its principal place of business at 200 CentrePort Drive, Suite 350, Greensboro, NC 27409; and

RAGBÖX PLATFORM SERVICES, a Delaware limited liability company ("Processor"), with its principal place of business at 1200 Brickell Avenue, Suite 2100, Miami, FL 33131.

This DPA supplements and is incorporated into the Master Services Agreement dated January 5, 2026, between the Parties (the "MSA"). In the event of a conflict between this DPA and the MSA, this DPA shall prevail with respect to data processing matters.

1. DEFINITIONS

1.1 "Personal Data" means any information relating to an identified or identifiable natural person, including Protected Health Information ("PHI") as defined by HIPAA, and personal data as defined under GDPR, CCPA, and other applicable data protection laws.

1.2 "Processing" means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, erasure, or destruction.

1.3 "Data Subject" means the identified or identifiable natural person to whom the Personal Data relates.

1.4 "Sub-Processor" means any third party engaged by Processor to process Personal Data on behalf of Controller.

1.5 "Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

2. SCOPE AND PURPOSE OF PROCESSING

2.1 Subject Matter. Processor shall process Personal Data on behalf of Controller solely for the purpose of providing the services described in the MSA, including: (a) document ingestion, OCR processing, and text extraction; (b) embedding generation and vector storage for retrieval-augmented generation; (c) AI-assisted query processing and response generation; and (d) audit logging and compliance reporting.

2.2 Categories of Data. The Personal Data processed under this DPA may include: (a) patient names, dates of birth, and medical record numbers; (b) clinical notes, diagnostic codes, and treatment plans; (c) insurance information and billing records; (d) employee names, contact information, and professional credentials; and (e) metadata associated with document processing.

2.3 Duration. Processing shall continue for the duration of the MSA, plus ninety (90) days for orderly data return or deletion.

3. OBLIGATIONS OF PROCESSOR

3.1 Processing Instructions. Processor shall process Personal Data only in accordance with Controller's documented instructions. If Processor believes that any instruction would violate applicable data protection law, Processor shall immediately inform Controller.

3.2 Confidentiality. Processor shall ensure that all personnel authorized to process Personal Data are

bound by written obligations of confidentiality and have received appropriate training in data protection.

3.3 Security Measures. Processor shall implement and maintain appropriate technical and organizational security measures, including: (a) AES-256 encryption at rest for all stored Personal Data; (b) TLS 1.3 encryption in transit; (c) role-based access controls with multi-factor authentication; (d) SOC 2 Type II certified infrastructure; (e) automated intrusion detection and monitoring; (f) regular vulnerability scanning and penetration testing; and (g) secure data backup with geographic redundancy.

3.4 Data Minimization. Processor shall process only the minimum amount of Personal Data necessary to fulfill the processing purposes described herein.

4. SUB-PROCESSING

4.1 Prior Authorization. Processor shall not engage any Sub-Processor without the prior written consent of Controller. Controller hereby approves the Sub-Processors listed in Annex B.

4.2 Sub-Processor Obligations. Processor shall ensure that each Sub-Processor is bound by data protection obligations no less protective than those set forth in this DPA.

4.3 Approved Sub-Processors. The following Sub-Processors are approved as of the Effective Date:

- Google Cloud Platform (Infrastructure hosting, US regions only)
- Cloud SQL for PostgreSQL (Database storage, us-east4)
- Vertex AI (AI model inference, no data retention)

4.4 Changes. Processor shall provide Controller with thirty (30) days' prior written notice before adding or replacing any Sub-Processor. Controller may object within fifteen (15) days on reasonable data protection grounds.

5. DATA SUBJECT RIGHTS

Processor shall promptly assist Controller in responding to requests from Data Subjects exercising their rights under applicable data protection law, including rights of access, rectification, erasure, data portability, and objection to processing. Processor shall respond to Controller's requests within five (5) business days.

6. DATA BREACH NOTIFICATION

6.1 Notification. In the event of a Data Breach, Processor shall notify Controller without undue delay, and in any event within twenty-four (24) hours of becoming aware of the breach.

6.2 Information. The notification shall include: (a) a description of the nature of the breach; (b) the categories and approximate number of Data Subjects affected; (c) the likely consequences of the breach; (d) the measures taken or proposed to address the breach; and (e) the contact details of the Processor's data protection officer.

6.3 Cooperation. Processor shall cooperate fully with Controller in investigating and remediating the breach and in meeting any applicable regulatory notification obligations.

7. PAYMENT TERMS

7.1 Processing Fees. Controller shall pay Processor the processing fees set forth in the MSA. The current fee schedule provides for: (a) platform subscription of Eight Thousand Five Hundred Dollars (\$8,500.00)

per month; (b) per-document processing fee of \$0.15 per page for OCR and extraction; (c) query processing at \$0.02 per query; and (d) storage at \$0.50 per GB per month.

7.2 Audit Costs. Each Party shall bear its own costs in connection with audits conducted under Section 8, unless an audit reveals a material breach by Processor, in which case Processor shall bear the reasonable costs of the audit.

7.3 Data Return/Deletion Costs. The costs of data return or deletion upon termination shall be borne by Controller, not to exceed Five Thousand Dollars (\$5,000.00).

8. AUDITS AND COMPLIANCE

8.1 Audit Rights. Controller shall have the right to audit Processor's compliance with this DPA, including inspections of Processor's facilities and systems, upon thirty (30) days' prior written notice and during normal business hours.

8.2 Certifications. Processor shall maintain SOC 2 Type II certification and shall provide Controller with copies of the most recent audit report upon request.

8.3 HIPAA Compliance. To the extent Processor processes PHI on behalf of Controller, the Parties shall enter into a Business Associate Agreement ("BAA") that complies with HIPAA and the HITECH Act.

9. INDEMNIFICATION

9.1 Indemnification by Processor. Processor shall indemnify, defend, and hold harmless Controller from any losses, damages, fines, penalties, and reasonable expenses (including attorneys' fees) arising from: (a) Processor's breach of this DPA; (b) Processor's processing of Personal Data in violation of Controller's instructions or applicable law; or (c) any Data Breach caused by Processor's failure to implement adequate security measures.

9.2 Limitation. Processor's aggregate liability under this DPA shall not exceed two (2) times the annual fees paid by Controller under the MSA, except in cases of willful misconduct or gross negligence.

10. TERMINATION AND DATA RETURN

10.1 Termination. This DPA shall terminate upon the termination or expiration of the MSA.

10.2 Data Return. Upon termination, Processor shall, at Controller's election: (a) return all Personal Data to Controller in a commonly used, machine-readable format within thirty (30) days; or (b) securely delete all Personal Data and certify such deletion in writing.

10.3 Survival. The confidentiality and security obligations of this DPA shall survive termination for a period of three (3) years.

11. GOVERNING LAW AND JURISDICTION

11.1 Governing Law. This DPA shall be governed by and construed in accordance with the laws of the State of North Carolina.

11.2 Jurisdiction. Any dispute arising under this DPA shall be resolved in the state or federal courts located in Guilford County, North Carolina.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first written above.

MEDCORE ANALYTICS INC. (Controller)

By: _____
Name: Dr. Sarah L. Wainwright
Title: Chief Privacy Officer
Date: _____

RAGBÖX PLATFORM SERVICES (Processor)

By: _____
Name: David Hurtado
Title: Chief Executive Officer
Date: _____