HIPAA BUSINESS ASSOCIATE AGREEMENT

Effective Date: October 09, 2025

This HIPAA Business Associate Agreement (the "Agreement") is entered into as of [Effective Date], by and between [Covered Entity Name], a [state of organization] [entity type] ("Covered Entity"), and **Root Data AI**, a Delaware limited liability company ("Business Associate").

RECITALS

A. Covered Entity and Business Associate are parties to one or more agreements pursuant to which Business Associate provides Dental AI Business Intelligence SaaS services to Covered Entity (collectively, the "Underlying Agreement").

B. In connection with the Underlying Agreement, Business Associate may create, receive, maintain, or transmit Protected Health Information on behalf of Covered Entity.

C. Covered Entity is a "covered entity" as defined under HIPAA.

D. The parties enter this Agreement to comply with HIPAA, the HITECH Act, and the HIPAA Regulations regarding PHI use and disclosure.

NOW, THEREFORE, the parties agree as follows:

1. DEFINITIONS

Terms used but not defined herein have the meanings in the HIPAA Regulations.

(a) "Breach" means the definition in 45 C.F.R. § 164.402.

(b) "Electronic Protected Health Information" or "ePHI" means the definition in 45 C.F.R. § 160.103.

(c) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

(d) "HIPAA Regulations" means regulations under HIPAA, including Privacy Rule (45 C.F.R. Parts 160, 164 Subparts A, E), Security Rule (45 C.F.R. Parts 160, 164 Subparts A, C), Breach Notification Rule (45 C.F.R. Parts 160, 164 Subpart D), and Enforcement Rule (45 C.F.R. Parts 160, 164 Subparts A, B, D, E).

(e) "HITECH Act" means Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

(f) "Protected Health Information" or "PHI" means the definition in 45 C.F.R. § 160.103, limited to information created, received, maintained, or transmitted by Business Associate for Covered Entity.

(g) "Required by Law" means the definition in 45 C.F.R. § 164.103.

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

(i) "Security Incident" means the definition in 45 C.F.R. § 164.304.

(j) "Unsecured Protected Health Information" means the definition in 45 C.F.R. § 164.402.

2. OBLIGATIONS OF BUSINESS ASSOCIATE

(a) Permitted Uses and Disclosures. Business Associate may use or disclose PHI only as permitted or required by this Agreement or Required by Law, including to perform services under the Underlying Agreement, provided it would not violate HIPAA Regulations if done by Covered Entity.

(b) Specific Uses and Disclosures. Business Associate may:

(i) Use PHI for its proper management, administration, or legal responsibilities.

(ii) Disclose PHI for its proper management, administration, or legal responsibilities if Required by Law or with reasonable assurances from the recipient for confidentiality and breach notification.

(iii) Use PHI for data aggregation as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

(iv) De-identify PHI per 45 C.F.R. § 164.514(a)-(c) for analytics, with de-identified data remaining Covered Entity's property.

(c) Prohibitions. Business Associate shall not use or disclose PHI for marketing, fundraising, or sale without Covered Entity's written consent.

(d) Safeguards. Business Associate shall implement administrative, physical, and technical safeguards to protect PHI confidentiality, integrity, and availability, complying with the Security Rule. These safeguards are detailed in **Exhibit A: HIPAA Compliance Summary for Root Data Platform on Microsoft Azure**, incorporated herein by reference.

(e) Reporting. Business Associate shall report any impermissible use/disclosure, Security Incident, or Breach of Unsecured PHI to Covered Entity without unreasonable delay, no later than 10 days after discovery, including details required by HIPAA.

(f) Mitigation. Business Associate shall mitigate harmful effects from violations.

(g) Subcontractors. Business Associate shall ensure that any subcontractors or sub-processors (including cloud service providers and AI services such as Microsoft Azure OpenAI / Azure AI Foundry) that create, receive, maintain, or transmit PHI on behalf of Business Associate agree in writing to the same restrictions and conditions that apply to Business Associate under this Agreement with respect to such PHI. Business Associate shall provide Covered Entity with notice of any material new or changed sub-processors that will have access to PHI.

(h) Access to PHI. Business Associate shall provide PHI access in a Designated Record Set to Covered Entity or Individuals per 45 C.F.R. § 164.524.

(i) Amendment of PHI. Business Associate shall amend PHI in a Designated Record Set per Covered Entity directions under 45 C.F.R. § 164.526.

(j) Accounting of Disclosures. Business Associate shall document disclosures for Covered Entity's response to Individual requests per 45 C.F.R. § 164.528.

(k) Availability of Records. Business Associate shall make practices, books, and records available to the Secretary for compliance determination.

(l) Return or Destruction. Upon termination, Business Associate shall return or destroy PHI; if infeasible, extend protections and limit uses.

3. OBLIGATIONS OF COVERED ENTITY

(a) Notify Business Associate of privacy practice limitations affecting PHI use/disclosure.

(b) Notify of changes or revocations in Individual permissions.

(c) Notify of agreed restrictions per 45 C.F.R. § 164.522.

4. TERM AND TERMINATION

(a) Term. Effective from Effective Date, terminates when all PHI is returned/destroyed or protections extended.

(b) Termination for Cause. Covered Entity may terminate upon material breach, providing cure opportunity; if uncured, terminate and report to Secretary if needed.

(c) Effect of Termination. Return/destroy PHI except where infeasible.

5. INDEMNIFICATION

Business Associate shall indemnify, defend, and hold harmless Covered Entity and its officers, directors, employees, agents, and affiliates from and against any and all claims, demands, actions, suits, proceedings, losses, damages, liabilities, costs, and expenses (including reasonable attorneys' fees and costs) arising out of or relating to any breach of this Agreement or any violation of HIPAA or other applicable law by Business Associate, its subcontractors, or agents.

The obligations under this Section shall survive the termination or expiration of this Agreement.

6. MISCELLANEOUS

(a) Regulatory References. References to HIPAA Regulations include amendments.

(b) Amendment. Amend as necessary for compliance.

(c) Survival. Section 2(l) obligations survive termination.

(d) Interpretation. Resolve ambiguities for HIPAA compliance.

(e) Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Delaware, without regard to its conflict of laws principles.

(f) No Third-Party Beneficiaries. No rights conferred on others.

(g) Counterparts. Executable in counterparts.

IN WITNESS WHEREOF, the parties execute this Agreement.

COVERED ENTITY:

Name: _____

Title: _____

Signature: _____

Date: _____

BUSINESS ASSOCIATE: Root Data AI

Name: _____

Title: _____

Signature: _____

Date: _____

EXHIBIT A

HIPAA Compliance Summary for Root Data Platform on Microsoft Azure

1. Business Associate Agreement (BAA) Coverage

Root Data qualifies as a business associate under HIPAA, providing services to covered entities in the dental and healthcare sector.

We operate under a valid Azure Plan subscription through Microsoft for Startups, with monthly billing in place. Azure for Startups operates under the Microsoft Customer Agreement (MCA), which automatically incorporates the HIPAA Business Associate Agreement (BAA) for eligible customers handling protected health information (PHI). As per Microsoft's Product Terms and Data Protection Addendum (DPA), the HIPAA BAA is automatically incorporated into our licensing agreement. No separate BAA signature is required.

This means our use of Azure services is contractually covered under HIPAA, provided we implement appropriate safeguards and operate as a covered entity or business associate.

Reference: HIPAA Compliance on Azure

2. Covered Azure Services

All services used in our platform are listed under Microsoft's HIPAA-covered offerings, as part of the in-scope "Azure and Azure Government" platform:

- Azure App Service (Premium)
- Azure Functions (Dedicated plan)
- Azure Storage (with private endpoints)
- Azure PostgreSQL Flexible Server
- Azure Cache for Redis
- Azure Key Vault
- Azure Monitor & Log Analytics
- Microsoft Entra ID (formerly Azure AD)

3. Technical Safeguards

Identity & Access

- RBAC-based access control integrated with a React + Next.js frontend
- Authentication follows OAuth2/OpenID Connect standards
- Role-based privilege mapping enforced via Microsoft Entra ID
- Secrets and credentials stored securely in Azure Key Vault

Network Security

- VNet integration for all web-accessible components
- NSG rules restrict outbound traffic to Redis, PostgreSQL, and Storage
- Private endpoints for Storage and Redis ensure PHI never traverses public networks

Data Storage & Sync

- Azure Storage for blob checkpointing and function runtime state
- Azure PostgreSQL Flexible Server for structured dental data
- Azure Cache for Redis for transient sync state and performance

Web Access & Sync Logic

- Web-accessible endpoints handle sync orchestration and API integration
- Sync logic built in Python, triggered via timers and HTTP endpoints
- GitHub Actions used for CI/CD with secure deployment to App Service

Open Dental API Integration

- Sync jobs ingest dental data via Open Dental API
- API credentials stored securely in Key Vault
- Data normalized and persisted in PostgreSQL with audit logging enabled

3.5 AI Features and Azure AI Services

Root Data's AI Coach and chat functionality may process limited practice data, including financial, operational, and in some cases patient-related financial information, to generate insights and answer user queries.

When a user interacts with the AI chat, Root Data only sends the minimum necessary context to Microsoft Azure OpenAI / Azure AI Foundry services **after obtaining explicit permission from the user within the application**. All such processing occurs within Microsoft's HIPAA-compliant infrastructure under the Microsoft Data Protection Addendum, which incorporates a Business Associate Agreement for eligible Azure services.

Root Data does not use customer data to train foundation models. Data sent to Azure AI services is used solely to fulfill the user's query and is subject to Microsoft's privacy and security commitments.

4. Compliance Controls

- Azure Policy initiative for HIPAA enforced across all resources
- Documented exemptions with compensating controls (e.g., client certificate policy for Function App)
- Diagnostic logs routed to Log Analytics for audit trail and monitoring
- SCM endpoint configured to allow secure GitHub Actions deployment without exposing app runtime

5. Licensing Evidence

Azure Plan subscription under "Root Data AI" is active and paid monthly. Invoices available upon request via the Azure portal or Microsoft billing support, confirming ongoing compliance with the incorporated HIPAA BAA under the Microsoft Customer Agreement.