SIMPLEST HEALTHCARE INC.

operating as

CoralEHR

Business Associate Agreement

Pursuant to the Health Insurance Portability & Accountability Act of 1996

45 CFR Parts 160 and 164

CONFIDENTIAL

BUSINESS ASSOCIATE AGREEMENT

Effective Date: _____

This Business Associate Agreement ("Agreement") is entered into by and between:

Covered Entity: _____
("Covered Entity" or "Practice")
Address: _____
Contact: _____

Business Associate: Simplest Healthcare Inc., operating as CoralEHR
("Business Associate")
Address: _____
Contact: _____

(each a "Party" and collectively the "Parties")

1. Purpose

Covered Entity has engaged Business Associate to provide cloud-based electronic health record (EHR) services, including clinical documentation, patient management, assessment administration, treatment planning, billing facilitation, and related functionality (the "Services"). In connection with the Services, Business Associate may create, receive, maintain, or transmit Protected Health Information ("PHI") on behalf of Covered Entity.

This Agreement sets forth the terms and conditions pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and their implementing regulations at 45 CFR Parts 160 and 164 (the "HIPAA Rules").

2. Definitions

Capitalized terms used in this Agreement and not otherwise defined shall have the meanings ascribed to them under the HIPAA Rules. Key definitions include:

- **Protected Health Information (PHI)** — Individually identifiable health information transmitted or maintained in any form, as defined in 45 CFR § 160.103.
- **Electronic Protected Health Information (ePHI)** — PHI transmitted or maintained in electronic media, as defined in 45 CFR § 160.103.
- **Breach** — The acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of such information, as defined in 45 CFR § 164.402.

- **Security Incident** — The attempted or successful unauthorized access, use, disclosure, modification, or destruction of ePHI, or interference with system operations, as defined in 45 CFR § 164.304.
- **Designated Record Set** — A group of records maintained by or for a Covered Entity, as defined in 45 CFR § 164.501.
- **Subcontractor** — A person to whom Business Associate delegates a function, activity, or service involving PHI.
- **Individual** — The person who is the subject of the PHI, as defined in 45 CFR § 160.103.

3. Obligations of Business Associate

3.1 Permitted Uses and Disclosures

Business Associate shall not use or further disclose PHI other than as permitted or required by this Agreement or as required by law. Business Associate shall use PHI solely to provide the Services described herein, including:

- Hosting, storing, and processing clinical records in FHIR R4-compliant data stores
- Enabling clinical note creation, assessment administration, and treatment plan management
- Facilitating secure clinician authentication and access control
- Processing de-identified billing metadata (no PHI is transmitted to payment processors)

3.2 Safeguards

Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI, in accordance with 45 CFR Part 164, Subpart C. These include, but are not limited to:

Administrative Safeguards:

- Designated security officer responsible for HIPAA compliance
- Workforce access management with role-based access controls
- Security awareness and training for all personnel with access to ePHI
- Documented policies and procedures for PHI handling, reviewed annually

Technical Safeguards:

- AES-256 encryption for ePHI at rest
- TLS 1.2+ encryption for all ePHI in transit
- Multi-factor authentication (MFA) required for all clinician accounts
- Automatic session termination and secure token management

- Audit logging of all access to ePHI
- Unique user identification and authentication via AWS Cognito

Physical Safeguards:

- PHI hosted exclusively on HIPAA-eligible AWS infrastructure (HealthLake, Lambda, API Gateway, Cognito, S3, DynamoDB)
- AWS maintains BAA coverage and SOC 2 Type II certification for in-scope services
- No PHI stored on local devices or endpoints; all processing occurs server-side

3.3 Minimum Necessary Standard

Business Associate shall limit its use, disclosure, and requests for PHI to the minimum necessary to accomplish the intended purpose, in accordance with 45 CFR § 164.502(b) and § 164.514(d).

3.4 Breach and Incident Reporting

Business Associate shall report to Covered Entity:

- Any use or disclosure of PHI not provided for by this Agreement, of which Business Associate becomes aware, within **five (5) business days** of discovery.
- Any Security Incident of which Business Associate becomes aware, within **five (5) business days** of discovery.
- Any Breach of Unsecured PHI, without unreasonable delay and no later than **thirty (30) calendar days** after discovery, in accordance with 45 CFR § 164.410.

Such reports shall include, to the extent available:

(a) The nature of the Breach or unauthorized use/disclosure

(b) The types of PHI involved

(c) The identity of the individuals affected

(d) Steps taken to mitigate harm

(e) Corrective actions implemented or planned

3.5 Subcontractors

Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees to the same restrictions, conditions, and requirements that apply to Business Associate under this Agreement, in accordance with 45 CFR § 164.502(e)(1)(ii) and § 164.308(b)(2).

Current Subprocessors:

Subprocessor	Services	PHI Processed	BAA Status
Amazon Web Services	Infrastructure (HealthLake, Lambda, API Gateway, Cognito, S3, DynamoDB, SES)	Yes	Active
Stripe, Inc.	Payment processing	No (de-identified UUIDs only)	N/A
Anthropic	AI-assisted clinical features	Configurable	Pending

Business Associate shall notify Covered Entity of any material changes to its Subprocessors at least **thirty (30) days** prior to such change.

3.6 Access to PHI

Business Associate shall make available PHI in a Designated Record Set to Covered Entity, or at the direction of Covered Entity to an Individual, within **fifteen (15) business days** of request, to satisfy Covered Entity's obligations under 45 CFR § 164.524.

3.7 Amendment of PHI

Business Associate shall make PHI available for amendment and incorporate amendments to PHI in a Designated Record Set at the direction of Covered Entity, within **fifteen (15) business days** of request, in accordance with 45 CFR § 164.526.

3.8 Accounting of Disclosures

Business Associate shall make available to Covered Entity the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528, within **thirty (30) days** of request.

3.9 Internal Practices and Government Access

Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services (HHS) for purposes of determining compliance with the HIPAA Rules.

3.10 De-identification

Business Associate shall not de-identify PHI or create limited data sets from PHI except as expressly authorized in writing by Covered Entity.

4. Obligations of Covered Entity

4.1 Notice of Privacy Practices

Covered Entity shall notify Business Associate of any limitations in its Notice of Privacy Practices under 45 CFR § 164.520, to the extent such limitations may affect Business Associate's use or disclosure of PHI.

4.2 Permission Changes

Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose PHI, to the extent such changes may affect Business Associate's permitted use or disclosure of PHI.

4.3 Restrictions on Use or Disclosure

Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI to which Covered Entity has agreed in accordance with 45 CFR § 164.522, to the extent such restriction may affect Business Associate's use or disclosure of PHI.

4.4 Permissible Requests

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity.

5. Permitted Uses and Disclosures by Business Associate

5.1 Service Performance

Business Associate may use or disclose PHI as necessary to perform the Services set forth in this Agreement or any underlying service agreement between the Parties.

5.2 Management and Administration

Business Associate may use PHI for its proper management and administration or to carry out its legal responsibilities, provided that any disclosure for such purpose is:

(a) Required by law; or

(b) Business Associate obtains reasonable assurances from the recipient that the PHI will be held confidentially and the recipient will notify Business Associate of any Breach of which it becomes aware.

5.3 Data Aggregation

Business Associate may use PHI to provide data aggregation services relating to the healthcare operations of Covered Entity, as permitted by 45 CFR § 164.504(e)(2)(i)(B).

5.4 Prohibited Uses

Business Associate shall **not**:

- Use or disclose PHI for marketing purposes without written authorization from the Individual
- Sell PHI, as defined in 45 CFR § 164.502(a)(5)(ii)
- Use or disclose genetic information for underwriting purposes, in accordance with the Genetic Information Nondiscrimination Act (GINA)

6. Term and Termination

6.1 Term

This Agreement shall become effective on the Effective Date and shall remain in effect for the duration of the underlying service relationship between the Parties, unless earlier terminated in accordance with this Section.

6.2 Termination for Cause

Either Party may terminate this Agreement if it determines that the other Party has materially breached this Agreement, provided that:

(a) The non-breaching Party provides written notice of the breach to the breaching Party;

(b) The breaching Party is given **thirty (30) calendar days** to cure the breach;

(c) If the breach is not cured within the cure period, the non-breaching Party may terminate this Agreement immediately upon written notice.

If cure is not feasible, the non-breaching Party may terminate this Agreement immediately upon written notice.

6.3 Effect of Termination

Upon termination of this Agreement for any reason, Business Associate shall:

(a) Return to Covered Entity or destroy all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, within **sixty (60) calendar days** of termination;

(b) Retain no copies of such PHI, except as required by law;

(c) Provide written certification of destruction to Covered Entity upon request.

If return or destruction of PHI is not feasible, Business Associate shall:

(a) Notify Covered Entity in writing of the conditions that make return or destruction infeasible;

(b) Extend the protections of this Agreement to such retained PHI;

(c) Limit further uses and disclosures to those purposes that make return or destruction infeasible, for so long as the PHI is retained.

7. CoralEHR Technical Security Specifications

7.1 Infrastructure

All ePHI is processed and stored within HIPAA-eligible AWS services in the US-East-2 (Ohio) region. Business Associate maintains an active Business Associate Agreement with Amazon Web Services, Inc. covering all in-scope services.

7.2 Data Standards

Patient data is structured in compliance with HL7 FHIR R4 (Fast Healthcare Interoperability Resources, Release 4), ensuring standardized clinical data representation and exchange capability.

7.3 Authentication and Access Control

All users are authenticated via AWS Cognito with mandatory multi-factor authentication. Session tokens are encrypted with AES-256 and stored in session-scoped storage that is automatically cleared upon browser session termination. Role-based access control ensures clinician-only access to clinical data.

7.4 Payment Processing Isolation

Payment processing is performed by Stripe, Inc. under PCI-DSS compliance. **No PHI is transmitted to Stripe** — only de-identified UUIDs, invoice amounts, and transaction metadata. Raw payment card data is handled exclusively by Stripe Elements and never touches Business Associate's servers.

8. Miscellaneous

8.1 Regulatory References

A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

8.2 Amendment

The Parties agree to take such action as is necessary to amend this Agreement from time to time for compliance with the HIPAA Rules and any other applicable law.

8.3 Survival

The respective rights and obligations of Business Associate under Sections 3 and 6.3 of this Agreement shall survive the termination of this Agreement.

8.4 Interpretation

Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

8.5 Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of _____ without regard to its conflict of laws provisions.

8.6 Entire Agreement

This Agreement, together with any underlying service agreement, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior negotiations, representations, or agreements relating thereto.

8.7 Notices

All notices required or permitted under this Agreement shall be in writing and delivered via email with read receipt or certified mail to the addresses set forth above.

9. Signatures

COVERED ENTITY

Signature: _____

Printed Name: _____

Title: _____

Date: _____

BUSINESS ASSOCIATE — Simplest Healthcare Inc.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

This agreement is based on the HHS Model Business Associate Agreement and 45 CFR § 164.504(e) requirements, tailored to CoralEHR's architecture. It should be reviewed by qualified legal counsel before execution.