BUSINESS ASSOCIATE AGREEMENT

HIPAA Compliance for Protected Health Information

Between:

BodyF1RST, Inc.
("Business Associate")

And:

[CUSTOMER NAME]
("Covered Entity")

Effective Date: [DATE]

RECITALS

WHEREAS, Business Associate provides corporate wellness services that may involve the creation, receipt, maintenance, or transmission of Protected Health Information (PHI) on behalf of Covered Entity;

WHEREAS, the parties desire to comply with HIPAA and HITECH;

NOW, THEREFORE, the parties agree as follows:

1. DEFINITIONS

Terms used in this Agreement have the same meaning as those in 45 C.F.R. Parts 160, 162, and 164.

"Protected Health Information" or "PHI" means individually identifiable health information as defined in 45 C.F.R. 160.103.

"Electronic PHI" or "ePHI" means PHI transmitted or maintained in electronic media.

"Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information.

"Breach" means acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule as defined in 45 C.F.R. 164.402.

2. PERMITTED USES AND DISCLOSURES

2.1 Service Performance. Business Associate may use or disclose PHI only as necessary to perform services specified in the Master Service Agreement.

2.2 Management and Administration. Business Associate may use PHI for proper management and administration if required by law or with reasonable confidentiality assurances.

2.3 De-Identification. Business Associate may de-identify PHI in accordance with 45 C.F.R. 164.514.

3. OBLIGATIONS OF BUSINESS ASSOCIATE

3.1 Not use or disclose PHI other than as permitted by this Agreement or required by law.

3.2 Implement administrative, physical, and technical safeguards to protect ePHI.

3.3 Limit PHI use, disclosure, or request to minimum necessary.

3.4 Report unauthorized use/disclosure, Security Incidents, and Breaches to Covered Entity.

3.5 Breach Notification. Notify Covered Entity of any Breach within **twenty-four (24) hours** of discovery.

3.6 Ensure subcontractors agree to same restrictions.

3.7 Make PHI available for individual access requests.

3.8 Incorporate amendments to PHI as directed.

3.9 Maintain accounting of disclosures.

3.10 Comply with HIPAA Security Rule.

3.11 Make records available to HHS for compliance determination.

4. SECURITY SAFEGUARDS

4.1 Administrative Safeguards:

Designated Security and Privacy Officers
Workforce security training
Access management policies
Incident response procedures
Risk assessments

4.2 Physical Safeguards:

SOC 2 certified data center access controls
Workstation security policies
Device and media controls

4.3 Technical Safeguards:

AES-256 encryption at rest
TLS 1.3 encryption in transit
Unique user identification
Automatic logoff
Audit controls
Multi-factor authentication

5. SUBCONTRACTORS

Subcontractor	Service	Compliance
Google Cloud Platform	Hosting & Storage	HIPAA BAA executed
Stripe	Payment Processing	HIPAA BAA executed
SendGrid	Email Communications	HIPAA BAA executed

6. TERM AND TERMINATION

6.1 This Agreement is effective upon the Effective Date and continues until MSA terminates.

6.2 Either party may terminate if other party materially breaches and fails to cure within 30 days.

6.3 Upon termination, Business Associate shall return or destroy all PHI, retain no copies unless legally required.

6.4 PHI obligations survive termination.

7. GENERAL PROVISIONS

7.1 This Agreement may be amended only in writing. Parties shall amend as necessary to comply with HIPAA changes.

7.2 This Agreement shall be interpreted consistently with HIPAA regulations.

7.3 Governed by federal law (HIPAA) and, to the extent not preempted, the laws of Texas.

SIGNATURES

BodyF1RST, Inc.

Signature: _____

Name: _____

Title: _____

[CUSTOMER NAME]

Signature: _____

Name: _____

Title: _____

Date: _____ Date: _____

This BAA is compliant with 45 CFR 164.504(e). Contact privacy@bodyf1rst.com for execution.