

COMPLIANCE · CONTRACT TEMPLATE

Business Associate Agreement (BAA)

Version 2 · Approved by CloudHealth Legal · Required for any client transmitting PHI.

This template is for redline use only. Final execution must be reviewed by CloudHealth Legal before signature. Do not modify the indemnification or HHS notification clauses.

1. Definitions

"PHI", "Breach", "Security Incident", "Covered Entity", and "Business Associate" carry the meanings set forth in 45 CFR §§ 160.103, 164.402, and 164.304.

2. Permitted Uses and Disclosures

1. Business Associate may use or disclose PHI only as necessary to perform the services set forth in the underlying Services Agreement.
2. Business Associate may use PHI for the proper management and administration of its business and to carry out its legal responsibilities.
3. Business Associate shall not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity.

3. Safeguards

Business Associate shall implement administrative, physical, and technical safeguards meeting the requirements of 45 CFR Part 164 Subpart C, including:

1. Encryption of PHI at rest (AES-256) and in transit (TLS 1.2+).
2. Role-based access controls with least-privilege defaults.
3. Annual workforce HIPAA training with documented attestation.

4. SOC 2 Type II controls maintained continuously.

4. Subcontractors

Business Associate shall ensure any subcontractor that creates, receives, maintains, or transmits PHI on its behalf agrees in writing to the same restrictions as this BAA.

5. Breach Notification

Business Associate shall notify Covered Entity within seventy-two (72) hours of discovering any Breach of Unsecured PHI. Notification shall include the nature of the breach, individuals affected, mitigation steps taken, and recommended remediation.

6. Term and Termination

This BAA is effective as of the Effective Date and continues until terminated by either party. Upon termination, Business Associate shall return or destroy all PHI received, except where return or destruction is infeasible, in which case protections shall extend until destruction is feasible.

7. HHS Access

Business Associate shall make its internal practices, books, and records available to the Secretary of HHS for purposes of determining compliance with the HIPAA Rules.

8. Indemnification

Each Party shall indemnify the other against losses arising from its own material breach of this Agreement, subject to the liability caps stated in the underlying Services Agreement.

9. Signature Block

Covered Entity: _____ Date: _____

Business Associate (CloudHealth, Inc.): _____ Date: _____