AccessHealthData — Business Associate Services Agreement (BASA)

Effective Date: Upon Customer's electronic acceptance

Between:

AccessHealthData, Inc. ("AccessHealthData"), a Business Associate under HIPAA
Customer ("Customer"), a Business Associate under HIPAA

Together, the "Parties."

---

1. Purpose and Scope

This Business Associate Services Agreement ("Agreement" or "BASA") governs AccessHealthData's creation, receipt, maintenance, transmission, and processing of Protected Health Information ("PHI") on behalf of Customer, who itself has one or more Business Associate relationships with Covered Entities or upstream Business Associates.

This Agreement is required under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, including the HITECH Act (collectively, "HIPAA").

This BASA applies solely to Customer's use of the AccessHealthData platform to ingest, normalize, store, transmit, or otherwise process PHI.

---

2. Definitions

2.1 "PHI"

Has the meaning given in 45 C.F.R. §160.103 and includes any Protected Health Information provided by Customer to AccessHealthData or obtained by AccessHealthData on Customer's behalf.

2.2 "ePHI"

PHI maintained or transmitted in electronic form.

2.3 "Business Associate"

Has the meaning specified in HIPAA. Customer affirms it is a Business Associate or a subcontractor to a Business Associate or Covered Entity.

2.4 "Services"

AccessHealthData's APIs, platforms, storage, normalization, and related infrastructure services.

3. Permitted Uses and Disclosures by AccessHealthData

AccessHealthData may use or disclose PHI only as follows:

3.1 To Provide the Services

To ingest, normalize, convert to FHIR, store, transmit, de-duplicate, retrieve, and otherwise process PHI as necessary to perform Services requested by Customer.

3.2 Management and Administration

As permitted under HIPAA for internal operations, including:

- security
- auditing
- platform maintenance
- troubleshooting
- logging
- fraud/abuse prevention

3.3 Legal Requirements

To comply with applicable laws, regulations, or lawful requests.

3.4 Minimum Necessary

AccessHealthData will use, disclose, and request only the minimum necessary PHI to deliver the Services.

4. Obligations of AccessHealthData

AccessHealthData shall:

4.1 Safeguards

Implement administrative, physical, and technical safeguards compliant with 45 C.F.R. §§164.308, 164.310, and 164.312 to protect PHI.

4.2 Reporting

Report to Customer any Security Incident or Breach involving PHI as required by 45 C.F.R. §164.410 without unreasonable delay.

4.3 Subprocessors

Ensure subcontractors who may access PHI enter into written agreements imposing the same restrictions and safeguards required herein.

4.4 Access Controls

Use role-based access, MFA, encryption at rest (AES-256) and in transit (TLS 1.2+), audit logs, and strict least-privilege policies.

4.5 Prohibition Beyond Scope

Not use or disclose PHI outside the scope of this Agreement.

4.6 Return or Destruction

Upon termination, return or securely destroy PHI as directed by Customer unless retention is required by law or infeasible.

5. Obligations of Customer

Customer shall:

5.1 Compliance

Comply with HIPAA to the extent required by Customer's relationships with Covered Entities and other Business Associates.

5.2 Permissions & Authority

Ensure it has authority (under upstream BAAs or CE agreements) to disclose PHI to AccessHealthData.

5.3 Minimum Necessary

Transmit only minimum necessary PHI to AccessHealthData.

5.4 User Authentication

Protect API keys, credentials, and access tokens, and ensure only authorized, trained personnel access PHI.

5.5 Misuse Notification

Notify AccessHealthData of any unauthorized use or disclosure of PHI involving Customer's systems or users.

6. Reporting and Breach Notification

6.1 Security Incidents

AccessHealthData maintains continuous monitoring and logs all significant security events. Routine, unsuccessful attempts at unauthorized access (e.g., port scans) are not reportable incidents.

6.2 Breach of Unsecured PHI

If AccessHealthData discovers a Breach of Unsecured PHI as defined by HIPAA, AccessHealthData will:

- Notify Customer without unreasonable delay (and no later than legally required)
- Provide details known at the time
- Cooperate with Customer's investigation
- Support notifications required under HIPAA Subpart D

7. Subcontractors and Subprocessors

AccessHealthData may use subcontractors (e.g., cloud infrastructure providers, logging systems, database vendors, OCR/normalization subprocessors). Each subprocessor that handles PHI must:

- sign a BAA or equivalent agreement
- implement safeguards meeting HIPAA standards

Customer consents to the use of AccessHealthData's subprocessors listed at www.accesshealthdata.com/subprocessors

8. Term and Termination

8.1 Term

This Agreement begins upon Customer's acceptance and remains in effect until terminated by either Party or until Customer's account is closed.

8.2 Termination for Cause

Either party may terminate this Agreement for a material breach if such breach is not cured within 30 days of written notice.

8.3 Effect of Termination

Upon termination:

- Customer may export all PHI via API
- AccessHealthData will, upon Customer request, securely destroy or return PHI
- AccessHealthData may retain backups if required by law or technically infeasible to remove, provided such retained data is safeguarded and not further used

9. Data Ownership

Customer retains all rights to PHI.

AccessHealthData does not obtain, assert, or claim ownership of PHI.

AccessHealthData may not de-identify PHI *without Customer's written permission.*

10. Security Practices Summary

AccessHealthData implements:

- Encryption at rest and in transit
- Role-based access & MFA
- Network segmentation
- Logging & anomaly detection
- Annual penetration testing
- Continuous vulnerability scanning
- Secure key management
- SOC2/HITRUST-aligned controls

11. Limitation of Liability

Except for obligations arising from gross negligence, willful misconduct, or violations of law, AccessHealthData's liability under this Agreement is limited in accordance with the liability provisions of the governing Terms of Service.

12. Governing Law

This Agreement is governed by the laws of the State of Delaware, excluding conflict-of-law rules.

13. Entire Agreement

This Agreement supplements and forms part of the Terms of Service. In case of conflict, this BASA controls with respect to PHI and HIPAA-related matters.

Acceptance Section

By clicking "Accept and Continue," Customer agrees to the terms of this Business Associate Services Agreement.