AIR360

Business Associate Agreement

Last updated: July 10, 2026

This Business Associate Agreement ("BAA") is entered into between Air360, Inc. ("Business Associate") and the customer identified in the applicable Order Form or Master Services Agreement ("Covered Entity" or "Customer").

This BAA supplements the parties' Services Agreement.

1. Purpose

Customer has requested this BAA to support its compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Air360 provides behavioral analytics and session replay software that is designed to operate without collecting Protected Health Information ("PHI") when configured according to Air360's implementation guidance.

The parties intend that Customer will configure and use the Services such that PHI is not transmitted to Air360.

This BAA governs the parties' respective obligations should PHI nevertheless be inadvertently transmitted to the Services.

Execution of this BAA does not authorize Customer to use the Services as a repository for PHI.

2. Definitions

Terms not otherwise defined shall have the meanings assigned under HIPAA, including:

- Protected Health Information (PHI)
- Breach
- Security Incident
- Unsecured PHI
- Business Associate
- Covered Entity
- Designated Record Set
- Secretary

3. Customer Responsibilities

Customer is solely responsible for configuring and using the Services in a manner that prevents the transmission of PHI.

Customer shall:

- enable masking of all text entry fields;
- exclude any page elements containing PHI from session replay;
- avoid transmitting PHI through URLs, query parameters, cookies, custom events, metadata, or custom properties;
- ensure that integrations with the Services do not transmit PHI;
- periodically review its implementation for continued compliance.

Customer shall not intentionally submit PHI to the Services.

4. Business Associate Responsibilities

If Business Associate inadvertently receives PHI, Business Associate shall:

- use appropriate administrative, physical, and technical safeguards to protect such information;
- not use or disclose PHI except as required to provide the Services or as required by law;
- report Breaches, Security Incidents, and unauthorized uses or disclosures as described in Section 8;
- cooperate with Customer regarding mitigation;
- securely delete or destroy inadvertently received PHI whenever reasonably practicable.

Business Associate does not intentionally collect, analyze, monetize, or otherwise use PHI.

5. Permitted Uses and Deletion

Air360 does not need or want to retain PHI. Any PHI inadvertently received shall not be used for any purpose other than to identify and delete it, or as required to comply with legal obligations.

Business Associate shall delete any inadvertently received PHI within twenty-four (24) hours of Customer's request, and in any event without unreasonable delay upon becoming aware of its receipt, except to the extent retention of specific data is required by applicable law.

Business Associate shall not use PHI for advertising, profiling, marketing, or any other secondary purpose.

6. Safeguards

Business Associate shall comply with the applicable requirements of the HIPAA Security Rule (45 CFR Part 164, Subpart C) with respect to electronic PHI, and shall maintain administrative, physical, and technical safeguards appropriate to the Services to protect any PHI inadvertently received.

As a technical safeguard, Business Associate enables full text obfuscation in session replay by default for Customer's account under this BAA, in addition to Customer's own masking and exclusion configuration.

7. Subcontractors

Business Associate shall require any subcontractor that may receive PHI to agree in writing to the same restrictions and conditions that apply to Business Associate under this BAA with respect to such PHI, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.314(a)(2)(iii).

8. Reporting and Breach Notification

Business Associate shall report to Customer, without unreasonable delay after discovery:

- any use or disclosure of PHI not provided for by this BAA;
- any Security Incident involving PHI;
- any Breach of Unsecured PHI, and in no case later than sixty (60) days after discovery, in accordance with 45 CFR 164.410.

Breach notifications shall include, to the extent known, a description of the breach, the types of PHI involved, and the steps Customer should take to protect against potential harm.

9. Individual Rights

The parties do not anticipate that Business Associate will maintain PHI in a Designated Record Set. To the extent Business Associate does maintain PHI in a Designated Record Set, Business Associate shall:

- make such PHI available to Customer as necessary for Customer to respond to individual access requests;
- incorporate amendments to such PHI as directed by Customer;
- make available the information required to provide an accounting of disclosures.

10. Availability to HHS

Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining compliance with HIPAA.

11. Return or Destruction

Upon termination of the Services, Business Associate shall securely delete any PHI inadvertently received within twenty-four (24) hours, unless retention is required by law.

12. Termination

This BAA terminates automatically upon termination of the Services Agreement.

Customer may also terminate this BAA and the Services Agreement if Business Associate materially breaches its obligations under this BAA, following the termination procedures in Section 11.2 of the Services Agreement.

13. Miscellaneous

If any provision of this BAA conflicts with HIPAA, HIPAA shall control.

This BAA supplements the Services Agreement and controls solely with respect to HIPAA obligations.

The limitation of liability set forth in Section 10 of the Services Agreement applies to this BAA.

This BAA is governed by the governing law and jurisdiction provisions in Section 12.6 of the Services Agreement.