

ACCUSIGHTS · BUSINESS ASSOCIATE AGREEMENT TEMPLATE

AccuSights Business Associate Agreement

The HIPAA business associate terms executed only when access to Protected Health Information is unavoidable for a specific engagement, with the AccuSights entity checked in the parties table.

VERSION

**Version 2026.10 — Effective
November 1, 2026**

CONTRACTING ENTITY

**AccuSights, Inc. or
AccuSights LLC (as checked)**

LEGAL TERMS

**accusights.com/legal
Security Through Compliance**

When this BAA is used. AccuSights' Services are designed to be performed without access to Protected Health Information. This BAA is executed only when PHI access is unavoidable for a specific engagement. Do not sign this BAA "just in case"; the AccuSights Terms of Service and the Protect Services Agreement each prohibit Customer from providing PHI until a BAA is in place.

This Business Associate Agreement ("**BAA**") is entered into as of the date of the last signature below (the "**BAA Effective Date**") between:

PARTY	ENTRY
Covered Entity / Upstream Business Associate ("Customer")	Legal name: _____ · State of organization: _____ · Entity type: _____ · Principal office: _____
Business Associate ("AccuSights")	☐ AccuSights, Inc. , a Delaware corporation ☐ AccuSights LLC , an Illinois limited liability company — in each case with its principal office at 2058 N. Western Ave, Chicago, IL 60647. <i>Check one only. This BAA binds only the entity checked; the other AccuSights entity is not a party and has no obligations under it.</i>
Underlying Agreement (the "Agreement")	☐ AccuSights Terms of Service Version 2026.10 and Order Form No. _____ (AccuSights, Inc.) ☐ AccuSights LLC Protect Services Agreement No. _____

AccuSights' HIPAA Compliance Officer and Privacy Officer is Dr. Kashmala Khalid, reachable at support@accusights.com with the subject "ATTN: HIPAA Compliance Officer".

1. Definitions

Capitalized terms used but not defined in this BAA have the meanings given in the HIPAA Rules. "**HIPAA Rules**" means the Privacy, Security, Breach Notification and Enforcement Rules at 45 C.F.R. Parts 160 and 164, as amended, including by the HITECH Act. "**PHI**" means Protected Health Information as defined at 45 C.F.R. § 160.103, limited to PHI that AccuSights creates, receives, maintains or transmits from or on behalf of Customer under the Agreement. "**Services**" means the services under the Agreement that require access to PHI, as described in Exhibit A.

2. Scope; Minimum Necessary; Permitted Uses and Disclosures

2.1 Scope limited to Exhibit A. AccuSights is a Business Associate of Customer only with respect to PHI accessed in performing the Services described in Exhibit A. Customer will not provide, and will configure the Services so as not to provide, PHI to AccuSights beyond that scope.

PHI that Customer provides outside the scope of Exhibit A, or that Customer provides in violation of the Agreement, is provided at Customer's sole risk and responsibility, although AccuSights will handle any such PHI it becomes aware of in accordance with this BAA.

2.2 Minimum necessary. Customer will request, and AccuSights will use, disclose and request, only the minimum PHI necessary to accomplish the intended purpose (45 C.F.R. § 164.502(b)). Customer will de-identify, redact or use limited data sets where the Services can be performed with them.

2.3 Permitted uses and disclosures. AccuSights may use and disclose PHI (a) as necessary to perform the Services; (b) for AccuSights' proper management and administration, provided that any disclosure is required by law or AccuSights obtains reasonable written assurances that the recipient will hold the PHI confidentially, use or further disclose it only as required by law or for the purpose disclosed, and notify AccuSights of any breach of confidentiality; (c) to provide Data Aggregation services relating to Customer's health care operations, if within the Services; (d) to de-identify PHI in accordance with 45 C.F.R. § 164.514(a)–(c), after which the de-identified data is not PHI and AccuSights may use it for any lawful purpose; and (e) as Required by Law.

2.4 Prohibited uses. AccuSights will not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Customer, except as permitted in Section 2.3(b) and (c), and will not Sell PHI or use it for marketing without the authorizations required by the HIPAA Rules.

3. Obligations of AccuSights

3.1 Safeguards. AccuSights will use appropriate administrative, physical and technical safeguards, and will comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided by this BAA.

3.2 Reporting. AccuSights will report to Customer (a) any use or disclosure of PHI not permitted by this BAA, (b) any Security Incident, and (c) any Breach of Unsecured PHI, in each case of which AccuSights becomes aware, **without unreasonable delay and in no case later than ten (10) business days after AccuSights' Discovery** of the Breach or non-permitted use or disclosure. The report will include, to the extent known, the information required by 45 C.F.R. § 164.410(c), and AccuSights will supplement it as information becomes available. The parties agree that this Section constitutes notice of, and no further reporting is required for, unsuccessful Security Incidents such as pings, port scans, blocked intrusion attempts and failed logins that do not result in unauthorized access to PHI.

3.3 Customer's notification responsibilities. Customer, as Covered Entity (or as upstream Business Associate), is solely responsible for determining whether a reportable Breach has occurred, for performing the risk assessment under 45 C.F.R. § 164.402(2), and for all notifications to Individuals, the Secretary, the media and any other person, and for their cost, subject to Section 6.

3.4 Subcontractors. AccuSights will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on behalf of AccuSights agrees in writing to restrictions and conditions at least as restrictive as those that apply to AccuSights under this BAA, in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2).

Customer consents to AccuSights' use of the Subprocessors listed in the AccuSights Data Processing Addendum as Subcontractors to the extent they access PHI.

3.5 Access. Within fifteen (15) business days after Customer's written request, AccuSights will make PHI in a Designated Record Set available to Customer so Customer can meet its obligations under 45 C.F.R. § 164.524. The parties acknowledge that the Services are not expected to involve Designated Record Sets unless Exhibit A states otherwise.

3.6 Amendment. Within fifteen (15) business days after Customer's written request, AccuSights will make PHI in a Designated Record Set available for amendment and incorporate amendments as directed by Customer under 45 C.F.R. § 164.526.

3.7 Accounting. AccuSights will document disclosures of PHI and related information required for Customer to respond to a request for an accounting under 45 C.F.R. § 164.528, and will provide that information to Customer within fifteen (15) business days after written request.

3.8 Requests from Individuals. If AccuSights receives a request directly from an Individual for access, amendment or accounting, AccuSights will forward it to Customer within five (5) business days and will not respond except to direct the Individual to Customer.

3.9 Customer's Privacy Rule obligations. To the extent AccuSights is to carry out one or more of Customer's obligations under Subpart E of 45 C.F.R. Part 164 (which the parties do not anticipate and which must be listed in Exhibit A to apply), AccuSights will comply with the requirements of Subpart E that apply to Customer in the performance of those obligations.

3.10 Books and records. AccuSights will make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining Customer's compliance with the HIPAA Rules, subject to attorney-client and other applicable privileges. AccuSights will notify Customer of any such request unless prohibited by law.

3.11 Not a Privacy or Security Official. AccuSights and its personnel do not serve as Customer's Privacy Official or Security Official (45 C.F.R. §§ 164.530(a)(1), 164.308(a)(2)) and do not perform Customer's risk analysis, breach risk assessments, workforce training or policy adoption on Customer's behalf unless expressly stated in Exhibit A as a Service, and then only as an advisory input to decisions made by Customer.

4. Obligations of Customer

4.1 Notices and restrictions. Customer will notify AccuSights in writing of (a) any limitation in Customer's notice of privacy practices, (b) any change in or revocation of an Individual's permission to use or disclose PHI, and (c) any restriction on use or disclosure agreed to by Customer under 45 C.F.R. § 164.522, in each case to the extent the limitation, change or restriction may affect AccuSights' use or disclosure of PHI.

4.2 Permissible requests. Customer will not request AccuSights to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Customer, except as permitted in Section 2.3(b) and (c).

4.3 Authority and minimization. Customer represents that it has the authority to disclose PHI to AccuSights for the Services, that it has obtained any required authorizations, and that it will provide PHI only as permitted by Section 2.

4.4 Security of Customer systems. Customer is responsible for the security of PHI on its own systems and in transit to and from the Services, for configuring the Services' security features, and for its workforce's access to the Services.

5. Term and Termination

5.1 Term. This BAA begins on the BAA Effective Date and continues until the earlier of (a) termination or expiration of the Agreement, (b) termination under Section 5.2, or (c) the date AccuSights no longer maintains any PHI and has returned or destroyed all PHI under Section 5.3.

5.2 Termination for cause. If either party determines that the other has materially breached this BAA, the non-breaching party will notify the breaching party in writing and provide thirty (30) days to cure. If the breach is not cured within that period, the non-breaching party may terminate this BAA and the portion of the Agreement that requires access to PHI. Termination of this BAA does not by itself terminate the Agreement as to Services that do not involve PHI.

5.3 Return or destruction. On termination, AccuSights will return to Customer or destroy all PHI in its possession, and retain no copies, within sixty (60) days, subject to the export window and deletion schedule in the Agreement. If return or destruction is infeasible (for example, PHI in backups pending rotation, or records AccuSights must retain by law), AccuSights will notify Customer of the conditions that make it infeasible, extend the protections of this BAA to the retained PHI, limit further uses and disclosures to the purposes that make return or destruction infeasible, and destroy the PHI when it becomes feasible (backups purged within ninety (90) days of termination in the ordinary course). On request, AccuSights will certify destruction in writing.

6. Relationship to the Agreement; Liability

6.1 Incorporation and precedence. This BAA is part of the Agreement. For PHI, this BAA controls over the Agreement and the Data Processing Addendum in case of conflict. For all other matters, the Agreement controls.

6.2 Liability cap incorporated. Each party's liability arising out of or related to this BAA is subject to the exclusions of damages and the limitations of liability in the Agreement, and the cap in the Agreement applies to liability under the Agreement and this BAA together, not separately. The costs of Breach notification, credit monitoring, call centers, forensics, public relations, regulatory fines and penalties, and third-party claims are excluded damages under the Agreement and are not recoverable under this BAA.

6.3 No indemnification. This BAA does not create any indemnification obligation on either party. The parties' indemnification obligations, if any, are solely those stated in the Agreement.

6.4 No third-party beneficiaries. Nothing in this BAA confers any right, remedy or claim on any person other than the parties, including any Individual.

6.5 Not an insurer. AccuSights is not an insurer of Customer's HIPAA compliance. Customer acknowledges that no safeguard eliminates the risk of a Security Incident and that Customer is responsible for maintaining cyber-liability insurance appropriate to its risk.

7. General

7.1 Regulatory references. A reference to a section of the HIPAA Rules means the section as in effect or as amended.

7.2 Amendment. The parties will negotiate in good faith to amend this BAA as necessary to comply with changes in the HIPAA Rules. Otherwise this BAA may be amended only in a writing signed by both parties.

7.3 Interpretation. Any ambiguity will be resolved to permit compliance with the HIPAA Rules. Nothing in this BAA requires AccuSights to take any action that would violate applicable law.

7.4 Survival. Sections 3.10, 5.3, 6 and 7 survive termination.

7.5 Governing law; venue. This BAA is governed by the laws of the State of Illinois, and the venue, jury-waiver and other dispute provisions of the Agreement apply.

7.6 Counterparts; electronic signature. This BAA may be executed electronically, including in the AccuSights Platform or via DocuSign, and in counterparts.

8. Signatures

CUSTOMER		ACCUSIGHTS (ENTITY CHECKED ABOVE)
Legal name		☐ AccuSights, Inc. ☐ AccuSights LLC
Typed name		Samad Khan
Title		Chief Executive Officer (of the entity checked)
Authority representation	☐ I am authorized to sign on behalf of Customer	
Signature	/s/ _____	/s/ _____
Date / UTC timestamp / record ID		

Exhibit A — Services Requiring PHI Access; Scope

ITEM	ENTRY
Agreement / Order Form / SOW reference	_____
Services requiring PHI access	_____ (for example: Protect SOC/MDR telemetry ingestion for endpoints in Customer's clinical environment; Comply HIPAA readiness evidence review of access logs containing patient identifiers)
Categories of PHI expected	_____ (for example: names and MRNs in log entries; file names; email metadata)
Systems / data sources in scope	_____
Data minimization measures	_____ (for example: log filtering; redaction; limited data set)
Designated Record Set involved?	☐ No ☐ Yes: _____
Privacy Rule obligations delegated to AccuSights (Section 3.9)	☐ None ☐ _____
Subcontractors with PHI access	Those Subprocessors on the DPA Subprocessor list that will access PHI for these Services: _____