Source: https://langfuse-docs-git-migrate-chatbot-ai-sdk-v7-langfuse.vercel.app/md-src/security/hipaa.md

HIPAA Compliance & Langfuse Business Associate Agreement (BAA)

Please find our BAA below. Langfuse Cloud is aligned with **HIPAA**, enabling healthcare organizations and partners to use Langfuse while adhering to the requirements of the Health Insurance Portability and Accountability Act (HIPAA). Langfuse offers a Business Associate Agreement (BAA) to cover the safeguarding of Protected Health Information (PHI). For questions regarding HIPAA compliance, please contact compliance@langfuse.com.

How to get set up on Langfuse HIPAA Cloud

1. You need a fresh Langfuse Cloud account on our HIPAA data region. *(Please note that this Langfuse instance is completely separate from our EU, US, and Japan data regions. Data migration is possible, please use the data migration cookbook)*
2. Sign up at hipaa.cloud.langfuse.com
3. Review BAA below
4. Upgrade to Pro plan or higher
5. BAA applies automatically
6. You're good to go!

Langfuse - Business Associate Agreement (BAA)

Latest revision: October 17th, 2025 | **download as PDF**

At a glance — This applies only if you're on our HIPAA Cloud with a HIPAA-eligible plan. It governs how we handle PHI: we act as your Business Associate under HIPAA, safeguard PHI with strict security and access controls, and only use it to run the Solution or as required by law. You stay responsible for configuring use correctly and limiting PHI to what's necessary. We notify you within 72 hours of any breach, help with regulatory obligations, and flow down the same protections to our subcontractors (with 30-day advance notice for any subprocessor changes). When the contract ends, we delete or return PHI (with limited exceptions for backups/legal holds). Liability follows the main contract.

Important Eligibility Notice

This Business Associate Agreement ('BAA') automatically applies only to Langfuse Client accounts that:

- are hosted in the Langfuse HIPAA Cloud Region at https://hipaa.cloud.langfuse.com; and
- are subscribed to a Pro, Teams, or Enterprise plan (each a 'HIPAA Eligible Plan').

Accounts that do not meet both conditions are not covered by this BAA and may not process Protected Health Information ('PHI') with Langfuse.

By provisioning or continuing to use an eligible account, the entity identified in the Langfuse billing records ('Client', 'Covered Entity' or its own business associate under HIPAA) is deemed to have read, understood and agreed to this BAA. No separate checkbox, click through or signature is required.

The current and past versions of this BAA are always available at https://langfuse.com/security/baa.

Questions? Email compliance@langfuse.com.

---

1. Parties & Incorporation

This BAA supplements and is incorporated by reference into the Langfuse Cloud Terms and Conditions (T&Cs), Order Form and/or any other written contract governing Client's use of the HIPAA eligible Langfuse Environment (collectively, the 'Main Contract').

Precedence. If there is a conflict on the same subject matter: (1) for PHI, the BAA controls; (2) for Personal Data (excluding PHI), the DPA controls; otherwise, the T&Cs control. Where information qualifies as both PHI and Personal Data, the BAA controls and the DPA applies only where not inconsistent with the BAA.

2. Definitions

Capitalized terms have the meanings set out in the U.S. Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160 & 164), as amended by the HITECH Act (together, 'HIPAA'). Key terms include:

Term	Meaning
PHI / Protected Health Information	Has the meaning in 45 C.F.R. §160.103 and is limited to information created, received, maintained or transmitted by Langfuse on

Term	Meaning
	behalf of Client.
Breach	As defined in 45 C.F.R. §164.402 — the unlawful acquisition, access, use or disclosure of Unsecured PHI.
Security Incident	As defined in 45 C.F.R. §164.304.
HITECH Act	Title XIII of the American Recovery and Reinvestment Act of 2009.

Other HIPAA terms (e.g., Designated Record Set, Unsecured PHI, Subcontractor) have the same meanings given in HIPAA.

Capitalized terms not defined here have the meanings set out in the Main Contract or in the DPA.

3. Permitted Uses & Disclosures

Langfuse may use or disclose PHI only:

- To provide the HIPAA Cloud Region environment and related support in accordance with the Main Contract;
- For our own management or legal obligations, provided any disclosure is (i) required by law or (ii) to a recipient that agrees to written confidentiality protections and promptly reports any breach; and
- As otherwise required by law.

Langfuse will not use or disclose PHI for any other purpose without Client's written instruction.

No De Identification Without Instruction. Langfuse will not use PHI to create de identified or aggregated datasets except (i) as expressly instructed in writing by Client or (ii) as required for security, fraud prevention, or legal compliance and only in accordance with 45 C.F.R. §164.514. For clarity, this restriction does not limit Langfuse's use of non PHI service telemetry permitted under the Main Contract.

4. Client Responsibilities

Client represents, warrants and agrees that:

- **Status.** Client is, and will remain, a Covered Entity or Business Associate under HIPAA and will comply with HIPAA in its use of the Services.
- **Minimum Necessary & Configuration.** Client will (a) limit PHI uploaded to the Service to the minimum necessary, (b) refrain from sending PHI via support tickets,

email, or non HIPAA workspaces, and (c) follow Langfuse documentation regarding encryption and other HIPAA configuration.

- **No Impermissible Requests.** Client will not request Langfuse to use or disclose PHI in a manner that would violate HIPAA if performed by Client.
- **Consents.** Client is responsible for obtaining any authorisations or consents required for Langfuse's uses and disclosures of PHI.

Langfuse may rely on Client's instructions when assessing the minimum necessary standard.

5. Safeguards

Langfuse will:

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI in accordance with the HIPAA Security Rule;
- Maintain a written information security program including risk assessments, encryption in transit and at rest, access controls, logging and vulnerability management; and
- Ensure that workforce members with access to PHI are bound by confidentiality obligations and trained on HIPAA requirements.

Data Location & Workforce Access. PHI is stored in the United States of America. Trained Langfuse workforce members may remotely access PHI from outside the United States solely as necessary to provide the Services and support, subject to least privilege access controls, MFA, logging, and confidentiality obligations. Langfuse will maintain appropriate contractual and technical safeguards for any such access.

Incorporation of TOMs. The technical and organizational measures in DPA Annex 2 are incorporated by reference and apply to PHI processed in the HIPAA Cloud. Langfuse may update the TOMs in accordance with the DPA, provided there is no material reduction in the overall level of protection for PHI.

6. Subcontractors

Langfuse will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on Langfuse's behalf agrees, in writing, to restrictions and security obligations at least as protective as those in this BAA and the HIPAA Security Rule.

Langfuse remains responsible for each Subcontractor's compliance and is liable for their acts and omissions relating to PHI to the same extent as if performed by Langfuse.

Langfuse maintains a public list of Subcontractors that Process PHI in the HIPAA Cloud at langfuse.com/security/subprocessors and will provide at least 30 days' prior email notice before adding or replacing any such Subcontractor. If Client reasonably objects on data protection grounds, Client may terminate the HIPAA Cloud subscription within that period and receive a pro rated refund of prepaid fees for the terminated remainder of the then current term.

7. Incident & Breach Reporting

Langfuse will:

- Report to Client any Breach of Unsecured PHI or unauthorized use or disclosure of PHI without unreasonable delay and in no event later than 72 hours after discovery;
- Report Security Incidents that materially compromise PHI; and
- Provide available information to assist Client in complying with 45 C.F.R. §§164.404–410.

Unsuccessful intrusion attempts (e.g., port scans, failed log ins, firewall pings) are commonplace and do not require notice under this section.

Cooperation. Following a Breach of Unsecured PHI, the parties will cooperate in good faith on investigation, risk assessment, and required notifications under 45 C.F.R. §§164.400–414. Each party's financial responsibility, if any, remains governed by the Main Contract (including any liability caps).

8. Individual Rights

To enable Client's obligations under 45 C.F.R. §164.528, Langfuse shall document and, upon written request, provide the information required by §164.528(b) for disclosures of PHI made by Langfuse that are subject to accounting under §164.528(a) (for example, excluding disclosures for treatment, payment, or health care operations; disclosures authorized by the individual; and incidental disclosures). Langfuse will provide this information within 15 business days of Client's written request. To the extent Langfuse maintains PHI in a Designated Record Set, Langfuse will assist Client with access (§164.524) and amendment (§164.526) within the timeframes required by HIPAA.

9. Books & Records

Langfuse will make its relevant policies, procedures and records relating to the security or use of PHI available to the U.S. Department of Health & Human Services upon request, subject to attorney client privilege and trade secret protections.

10. Term & Termination

Term. This BAA is coterminous with the Main Contract. It becomes effective automatically when Client first creates or upgrades an account that satisfies the eligibility criteria described in the Important Eligibility Notice and remains in effect until the termination of the Main Contract.

Termination for Breach. Either party may terminate this BAA immediately upon written notice if the other party materially breaches and the breach is not curable, or upon 30 days' written notice if curable and not cured within that period.

Return/Destruction of PHI. Upon termination, Langfuse will return or destroy PHI within 30 days. If any PHI is retained solely in immutable backups, system logs, or subject to legal hold, destruction may be infeasible until those media roll off in the ordinary course; Langfuse will not use or disclose such PHI for any purpose and will complete destruction within 90 days after roll off or release of hold.

Survival. Notwithstanding anything to the contrary, Langfuse's obligations under this BAA survive until all PHI provided by or on behalf of Client is returned or destroyed, and thereafter for so long as Langfuse retains any PHI because return or destruction is infeasible, in which case Langfuse will continue to protect such PHI and limit further uses/disclosures to those that make return or destruction infeasible.

11. Miscellaneous

- **No Third Party Beneficiaries.** Nothing in this BAA confers rights on anyone other than the parties.
- **Amendment.** Langfuse may update this BAA prospectively by posting a revised version and providing at least 30 days' notice. If Client objects to a material change that adversely affects it, Client may terminate the HIPAA Cloud subscription before the effective date and Langfuse will refund any prepaid fees for the period after termination.
- **Liability.** Each party's liability under this BAA is subject to the limitations in the Main Contract, except that HIPAA fines imposed due to a party's breach are borne by that party.
- **Governing Law.** Unless the Main Contract states otherwise, this BAA is governed by the same law and dispute forum as the Main Contract.
- **Notices.** Notices are governed by the Main Contract's notice clause.

Optional countersignature. *Upon Client's written request, Langfuse will provide a countersigned copy of this BAA for record-keeping. The effectiveness of this BAA does not depend on a separate signature.*

Old Versions of the Langfuse BAA

- Download Langfuse BAA, April 2025