LFW

Legal

Business Associate Agreement Template

Last updated November 14, 2026

Version 1.0, effective November 14, 2026. Unsigned template; execution and approval of the identified HIPAA environment are required. All legal documents (lfw.com/legal/). Download PDF (lfw.com/legal/lfw-business-associate-agreement-v1.0.pdf).

This unsigned template is for a specifically approved HIPAA environment only. It does not authorize PHI in the default shared service. **Before any PHI is received, complete all fields, validate the environment and downstream agreements, obtain licensed counsel's review and sign.**

1. Parties, scope and definitions

This Business Associate Agreement (BAA) is between **[Client's legal name, address and role as Covered Entity or upstream Business Associate]** (Client) and **LFW.com LLC, doing business as LFW** (Business Associate), effective **[Execution date]**. It supplements the MSA and Order Form **[Order identifier, services, HIPAA environment, hosting region, security exhibit and designated contacts]**.

HIPAA means the Health Insurance Portability and Accountability Act and applicable HITECH requirements and implementing regulations at 45 CFR Parts 160 and 164. Terms including Breach, Designated Record Set, Electronic PHI, Individual, Required by Law, Security Incident, Subcontractor and Unsecured PHI have their regulatory meanings. PHI here means information Business Associate creates, receives, maintains or transmits on Client's behalf in the identified services.

2. Permitted uses and disclosures

Business Associate may use and disclose PHI only as needed to perform the identified services on Client's documented instructions, as expressly permitted by this BAA, or as Required by Law. It will not use or disclose PHI in a way that would violate the Privacy Rule if done by Client, except where HIPAA permits a business associate to do so and this BAA expressly authorizes it. This template authorizes no sale, marketing, model training, independent analytics, data aggregation or de-identification for Business Associate's own purposes.

Business Associate will request, use and disclose only the minimum necessary PHI where that standard applies. No ordinary AI, messaging, payment or support integration may receive PHI unless approved for this environment and covered by the required downstream agreement. Client will not instruct an impermissible use or disclosure.

3. Safeguards and subcontractors

Business Associate will use appropriate safeguards to prevent unauthorized use or disclosure and comply with applicable requirements of the Security Rule for Electronic PHI. It will implement the risk analysis, risk management, workforce access controls, training, security policies, incident procedures and other measures required by HIPAA for its role. The signed security exhibit must describe the actual environment, backup and restoration arrangements and responsible parties; the general trust policies are not a substitute for that exhibit.

Before a subcontractor creates, receives, maintains or transmits PHI on Business Associate's behalf, Business Associate will obtain a written agreement imposing the same applicable restrictions, conditions and Security Rule requirements. It will take required steps to cure or end a known material subcontractor violation, and terminate the arrangement if cure is unsuccessful and termination is feasible. **Before activation, identify every PHI-handling host, storage, backup, communications, support and other subcontractor and verify signed BAAs.**

4. Reporting and mitigation

Business Associate will report impermissible uses or disclosures and Security Incidents to Client without unreasonable delay. It will notify Client within 24 hours of confirming an incident affecting Client's PHI, consistent with the Incident Response Plan. It will report a Breach of Unsecured PHI without unreasonable delay after discovery and within 24 hours after discovery; discovery includes what reasonable diligence would reveal under 45 CFR 164.410. The confirmation trigger does not postpone a discovery-based or earlier legal duty. A legally required delay under 45 CFR 164.412 applies.

The initial report will include available information, followed by prompt supplements: affected individuals, nature of the PHI, dates, what occurred, likely consequences, mitigation, protective steps and a contact. Business Associate will mitigate harmful effects to the extent practicable and cooperate with Client's risk assessment, documentation and required notices. Client is responsible for individual, HHS and media notices unless separately delegated in writing or law places a direct duty on Business Associate. This BAA does not replace statutory reporting duties.

Before signing, the parties must name primary and backup incident contacts and document a monitoring and escalation procedure capable of meeting these deadlines. This template does not add an unstated on-call support service.

5. Individual rights and government access

Business Associate will make PHI in a Designated Record Set available to Client or, as Client directs, to the Individual in the time and manner needed for Client to meet 45 CFR 164.524. It will make amendments as directed or agreed under 45 CFR 164.526 and incorporate them. It will record and provide information needed for an accounting of disclosures under 45 CFR 164.528. It will promptly forward direct individual requests to Client, unless Client has expressly delegated the response.

To the extent Business Associate performs Client's Privacy Rule duties, it will comply with the requirements applicable to those duties. It will make its internal practices, books and records relating to use and disclosure of PHI available to the Secretary of HHS for determining HIPAA compliance. A questionnaire-only audit provision does not restrict that access.

6. Client responsibilities

Client will notify Business Associate of privacy-notice limitations, changes or revocations of permission, and agreed restrictions that affect the services. Client determines lawful disclosure to Business Associate, necessary authorizations, its records schedule and which records comprise its Designated Record Set. Client will use only the approved HIPAA environment and approved integrations, with authorized users and required security controls. **Before signing, the parties must set operational response times for access, amendment and accounting requests and identify any delegated Client duties.**

7. Term, termination and PHI return

This BAA continues while Business Associate holds PHI for Client. Client may terminate the affected arrangement for a material breach of this BAA. Where cure is feasible, Client may allow a reasonable cure period consistent with HIPAA; a continuing violation that cannot be cured permits termination without waiting for the MSA's ordinary cure period.

On termination, at Client's choice Business Associate will return or destroy all PHI, including subcontractor-held copies, and retain no copies if feasible. If return or destruction is infeasible, it will explain why, continue this BAA's protections and limit use and disclosure to the purposes making return or destruction infeasible for as long as PHI is retained. Backup copies are included; no automatic backup exception permits unrelated use. Business Associate will confirm the disposition in writing. **Before signing, the parties must agree a feasible PHI return, destruction and backup-expiry plan.**

8. Relationship to other documents and signatures

This BAA controls conflicting agreement terms concerning PHI. Mandatory law controls; no liability limitation excuses a regulatory duty. The parties will amend it as needed to comply with HIPAA. The MSA's government-buyer priority applies subject to mandatory HIPAA duties. This template adds no new indemnity or insurance guarantee. The parties' counsel must review liability allocation, public-sector authority and any state health-privacy requirements. No third party receives contractual enforcement rights merely from this BAA.

Client authorized signatory: **[Name, title, signature and date]**

LFW.com LLC authorized signatory: **[Name, title, signature and date]**