Business Associate Agreement

Last Updated: July 27, 2026

This Business Associate Agreement, or "**BAA**," is part of the agreement between Customer and OneTrust (together, the "**Parties**"). In this BAA, we refer to that agreement as the "**Agreement**".

1. Definitions.

Unless this BAA defines a term differently, capitalized terms have the meanings given in HIPAA or the Agreement. Specifically, the terms Breach, Business Associate, Covered Entity, Designated Record Set, Electronic Health Record, Privacy Rule, and Security Incident have the meanings given in HIPAA.

"**BAA Services**" means the online software applications in the HIPAA environment that OneTrust provides as part of the Cloud Services.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, including the Privacy Rule, Security Rule, Enforcement Rule, and Breach Notification Rule at 45 CFR Parts 160 and 164, the Health Information Technology for Economic and Clinical Health Act ("**HITECH**"), and the Omnibus Rule, each as amended.

"**Protected Health Information**" or "**PHI**" means "protected health information" whether oral or recorded in any form or medium, to the extent the information is subject to HIPAA, that meets all of the following conditions: (a) relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; (b) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, as defined in 45 CFR §160.103; and (c) Customer uploads the information to the BAA Services.

"**Unsuccessful Security Incident**" means unsuccessful attempts (including pings, unsuccessful log-on attempts, denial of service attacks, port scans and attempts) for unauthorized access, use, disclosure, modification, or destruction of information, or interference with the general operation of OneTrust's systems or the BAA Services.

2. Applicability.

This BAA applies to the BAA Services only when Customer is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI, and OneTrust is therefore acting as a Business Associate or Subcontractor of a Business Associate under HIPAA. Customer will not share PHI with OneTrust outside the BAA Services. OneTrust has no liability for any PHI shared outside the BAA Services.

3. Scope of BAA Services.

Customer may upload PHI into the BAA Services. Customer is responsible for obtaining any consents or authorizations required to disclose PHI to OneTrust.

OneTrust, its subcontractors, and its subprocessors do not create PHI or provide data aggregation services in the provision of the BAA Services.

4. Permitted Uses and Disclosures of PHI.

OneTrust will only use and disclose PHI:

- to provide the BAA Services,
- as permitted by the Agreement,
- as required by law,
- that has been de-identified to provide Usage Data relating to the BAA Services, as permitted under 45 CFR §164.514(a)–(c).

OneTrust may also use and disclose PHI for the proper management and administration of OneTrust, or to carry out OneTrust's legal responsibilities as the Business Associate, but only if:

- the disclosure is required by law, or
- OneTrust obtains reasonable assurances from the recipient that the PHI will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed, and the recipient agrees to notify OneTrust of any breach of confidentiality of which it becomes aware.

To the extent required by 45 CFR §164.502(b) and 45 CFR §164.514(d), each Party will make reasonable efforts to limit its use, disclosure, and request of PHI to the minimum necessary to accomplish the intended purpose. Customer will not require OneTrust to use or disclose PHI in any manner that would violate HIPAA if done by Customer.

5. Safeguards.

OneTrust will use appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI as required under 45 CFR Part 160 and 45 CFR Part 164 Subparts A and C (the "**Security Rule**"), and to prevent the use or disclosure of PHI other than as permitted under the Agreement.

OneTrust LLC's Information Security Management System (ISMS) is ISO/IEC 27001:2022 and ISO/IEC 27017:2015 certified, and OneTrust LLC's Privacy Information Management System (PIMS) is ISO/IEC 27701:2019 certified. OneTrust LLC has completed a SOC 2 Type 2 report providing verification of security, confidentiality, and availability controls.

6. Notification.

OneTrust Responsibilities:

OneTrust will notify Customer of any Breach of PHI it discovers without unreasonable delay (no later than 60 calendar days) following discovery, in accordance with 45 CFR §164.410 (the "**Breach Notification Rule**"). This notification will include, to the extent possible, all information required under the Breach Notification Rule, including description of the Breach, types of information involved, mitigation steps taken, and any steps OneTrust recommends to address the Breach. OneTrust may delay notification if required by law or for law enforcement purposes.

OneTrust will promptly notify Customer of any Security Incident of which OneTrust becomes aware. OneTrust periodically experiences Unsuccessful Security Incidents. Unsuccessful Security Incidents are deemed reported by this BAA and do not require separate notice.

OneTrust will deliver notices under this Section 6 to the notification email address provided by Customer in the Agreement or to another Customer contact.

Customer Responsibilities:

Customer is solely responsible for determining whether to notify impacted individuals, determining if regulatory bodies, such as the Secretary of the U.S. Department of Health and Human Services ("**Secretary**"), or other enforcement commissions applicable to Customer need to be notified, and for providing any such notices.

7. Subcontractors and Subprocessors.

OneTrust may use subcontractors and subprocessors (collectively, "**Subcontractors**") to provide the BAA Services and Subcontractors may receive, maintain, or transmit PHI on OneTrust's behalf.

Before allowing a Subcontractor to receive, maintain, or transmit PHI on OneTrust's behalf, OneTrust will enter into a written agreement with that Subcontractor requiring it to protect the PHI and comply with restrictions and conditions that are no less protective than the restrictions and conditions that apply to OneTrust under this BAA, in accordance with 45 CFR §164.502(e)(1) and 45 CFR §164.504(e)(ii)(D).

Each Party's aggregate liability for one or more breaches of this BAA shall be subject to the limitations and exclusions of liability set out in the Agreement.

8. **Authorized Access, Amendment of PHI, and Accounting**.

To the extent OneTrust maintains PHI in a Designated Record Set and Customer cannot access that PHI directly through the BAA Services, OneTrust will make the PHI maintained by OneTrust or its Subcontractors in Designated Record Sets available to Customer for inspection and copying within 10 days of a request by Customer so Customer can meet its access and amendment obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.524 and §164.526. If OneTrust maintains an Electronic Health Record, OneTrust shall provide such information in electronic format to enable Customer to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. §17935(e). To the extent that a patient makes a request to OneTrust for a Designated Record Set or Electronic Health Record that OneTrust maintains on behalf of Customer, OneTrust shall forward such request to Customer within 10 calendar days of receipt and advise the patient that Customer will respond to the request. Customer agrees that it, and not OneTrust, is responsible for responding to the patient to fulfill its obligations under HIPAA.

Within 10 days of notice from Customer, OneTrust and its Subcontractors will make available to Customer, through the BAA Services, the information maintained by OneTrust that Customer reasonably needs to respond to a request for an accounting of disclosures under 45 C.F.R. §164.528 and the HITECH Act. OneTrust shall notify Customer within 5 business days of receipt of any request by an individual for an accounting of disclosures so Customer may fulfill its obligation to respond to such requests under the Privacy Rule and the HITECH Act.

Customer is solely responsible for responding to requests for accounting, access, or amendment.

9. **Restriction Agreements**.

OneTrust will comply with any agreement Customer enters into with an individual that restricts use or disclosure of PHI under 45 CFR §164.522(a) if the Parties agree in a signed writing to implement such restrictions. Customer will promptly notify OneTrust in writing if such a restriction is terminated or modified.

10. **Records**.

OneTrust will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary to determine Customer's compliance with HIPAA as required under 45 C.F.R. §164.504(e)(2).

11. **Deletion of PHI**.

When the Agreement or the applicable BAA Services end, OneTrust will destroy all PHI in OneTrust's possession unless retention is required by law. If destruction is infeasible, OneTrust will return the PHI to Customer or, where return is infeasible:

- continue to protect the retained PHI under this BAA, and
- limit further use and disclosure to those purposes that make return or destruction infeasible or that are otherwise required by law.

12. **Term and Termination**.

This BAA is in effect so long as Customer subscribes to the BAA Services, unless otherwise terminated or replaced in accordance with the Agreement.

13. **Liability**.

14. **Conflict of Laws and Order of Precedence**.

For any conflicts between this BAA and the Agreement, this BAA controls.

15. **No Third-Party Beneficiaries**.

Nothing express or implied in the Agreement or this BAA is intended to confer, nor shall anything herein confer upon any person other than Customer, OneTrust, and their respective successors or permitted assigns, any rights, remedies, obligations or liabilities whatsoever.

16. **Mitigation**.

In the event of a Breach resulting in the unauthorized use or disclosure of PHI in violation of this BAA, the Parties will, to the extent practicable under the circumstances, make commercially reasonable efforts to mitigate the harmful effects resulting from such Breach.

17. **Entire Agreement**.

This BAA supersedes any and all prior and contemporaneous business associate agreements or agreements between the Parties relating to PHI and constitutes the final and entire agreement between the Parties with respect to this subject matter.