



Business Associate Agreement

Last Updated: July 1, 2025

This Business Associate Agreement (“**BAA**”) supplements the agreement between Customer and OneTrust into which it is incorporated by reference (“**Agreement**”).

This BAA governs each Party’s respective obligations regarding Protected Health Information falling under the scope of HIPAA. In case of conflict between a provision of the Agreement and this BAA, the BAA shall prevail.

1. Definitions.

Unless otherwise defined below, all capitalized terms in this BAA shall have the meaning given to them in HIPAA or in the Agreement:

“**HIPAA**” means the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, including the Privacy Rule, Security Rule and Breach Notification Rule set forth at 45 CFR §§ 160 and 164, as well as the Health Information Technology for Economic and Clinical Health Act (“**HITECH**”), following modification and the Omnibus Rule.

“**Protected Health Information**” (or “**PHI**”) shall have the same meaning as the term “protected health information” in 45 CFR § 160.103 of HIPAA, limited to such PHI that is received, transmitted, or maintained by OneTrust on behalf of Customer as part of the Customer Content input into the BAA Services. “**BAA Services**” means the online software applications in the designated HIPAA Cloud Environment specifically set out in the Order Form (and further described in the OneTrust User Guide) provided by OneTrust as part of the Cloud Services.

2. Relationship of the parties and applicability.

For purposes of this BAA, Customer is acting as a Covered Entity and OneTrust is acting as a Business Associate. Customer warrants that it has full legal authority to enter into to this BAA and that it has obtained any consents and/or other legal authorizations required under HIPAA to disclose PHI to OneTrust.

3. Permitted use and disclosure of Personal Health Information.

OneTrust may receive, maintain, transmit, use, and disclose PHI on behalf of Customer to: (a) provide the Cloud Services and (b) as permitted under HIPAA, including (i) the proper management and administration of OneTrust and (ii) to carry out OneTrust’s legal responsibilities. Customer acknowledges that neither OneTrust nor its subcontractors and/or subprocessors “create” Protected Health Information in the provision of the Cloud Services.

OneTrust may disclose PHI for the purposes described above in subsection (b), provided that (i) the disclosure is required by law, or (i) OneTrust obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and that the person notifies OneTrust of any instances of which it is aware in which the confidentiality of the information has been breached. OneTrust may provide Data Aggregation services relating to Health Care Operations when specifically instructed to do so by Customer and limited to what is allowed under HIPAA. OneTrust may use de-identified information, as defined and under the requirements described in 164.514(a)-(c) HIPAA, to provide anonymized and aggregated statistics and analytics relating to the Cloud Services. Customer will not require OneTrust to use or disclose PHI in any way that is not allowed under HIPAA or under the Agreement. The Parties shall make reasonable efforts to limit the use and disclosure of PHI to what is necessary to accomplish the intended use, disclosure or request, including the provision of service governed by the Agreement.

4. Safeguards.

OneTrust undertakes to use appropriate administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of PHI, as required under the Security Rule of HIPAA. OneTrust LLC’s Information Security Management System (ISMS) is ISO/IEC 27001:2022 and ISO/IEC 27017:2015 certified.



OneTrust has completed a SOC 2 Type 2 report providing verification of the security, confidentiality, and availability controls maintained by OneTrust LLC and OneTrust Technology Limited. OneTrust LLC's Privacy Information Management System (PIMS) is ISO/IEC 27701:2019 certified.

5. Notification.

OneTrust shall notify Customer following the discovery of unauthorized use or disclosure of PHI without unreasonable delay and no later than 60 days after becoming aware of a breach. Any notification might be delayed if required for law enforcement purposes. Notification to individuals, public authorities and/or any other third parties shall be performed by Customer.

6. Subcontractors and Subprocessors.

OneTrust may engage subcontractors and/or subprocessors in connection with providing services to Customer under the Agreement and, in accordance with 45 CFR § 164.502(e)(1), such subcontractors and/or subprocessors may receive, maintain, transmit, use, and disclose PHI, provided OneTrust obtains satisfactory assurances in an agreement between OneTrust and each subprocessor that the subprocessor will appropriately safeguard the PHI in a manner no less restrictive than the terms in this BAA that apply to OneTrust with respect to such PHI.

7. Authorized access, amendment of PHI, and accounting.

By virtue of providing the Cloud Services, OneTrust will make available to Customer any PHI, in order for Customer to fulfil its obligations of providing access, amendment, and accounting under 45 CFR § 164.524, § 164.526, and § 164.526. Customer is ultimately responsible for appropriately responding to any such requests. OneTrust will not address or manage requests for access or amendment on behalf of Customer, nor provide accounting to individuals.

8. Records.

OneTrust will make its internal practices, books, and records relating to the use and disclosure of PHI received from, or received by, OneTrust on behalf of Customer, available to the Secretary for purposes of determining Customer's compliance with this subpart.

9. Return and Deletion of PHI.

Following termination or expiry of the Agreement, and unless otherwise provided by law, OneTrust shall return or destroy all PHI that OneTrust still maintains in any form and retain no copies of such PHI. If such return or destruction is not feasible, OneTrust will extend the protections of this BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

10. Customer Obligations.

Customer shall notify OneTrust of any changes in the permission by an individual to use or disclose their PHI to the extent that such changes may affect OneTrust's use or disclosure of PHI.

11. Termination and liability.

This BAA will expire upon the expiration term of the Agreement or earlier termination thereof. 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. In no event shall either party's liability for a breach of this BAA exceed the liability cap set out in the Agreement. Neither party limits or excludes any liability that cannot be limited or excluded under applicable law (such as for fraud).

12. Conflict of laws an Order of Precedence.

With respect to PHI, in the event of conflict between this BAA and any other privacy and security provisions in the Agreement, the provisions more protective of PHI shall prevail.