Effective starting: January 1st, 2025

Business Associate Agreement

This Business Associate Agreement (**"BAA"**) supplements the KnowBe4 Terms of Service, or separately signed agreement in place between Customer and KnowBe4 covering Customer's use of KnowBe4's Services (the **"Agreement"**), where applicable. The term "Customer" shall mean the organization entering into this BAA and shall include its Affiliates, as applicable. Unless otherwise defined in the body of this BAA or in the Agreement, all capitalized terms used in this BAA will have the meanings given to them in Section 1 of this DPA.

Customer is entering into this BAA with KnowBe4 as Customer is either a Covered Entity or a Business Associate under HIPAA and, as such, is required to enter into business associate contracts with certain processors that may have access to PHI. If there is any conflict between this BAA and/or the Agreement in respect of the parties' respective privacy and security obligations in respect of PHI, the terms of this BAA shall control.

1. DEFINITIONS. Capitalized words and phrases used in this BAA have the meanings given below or in HIPAA. If not defined below or in HIPAA, they have the meanings given in the Agreement.

Business Associate: the meaning given in 45 CFR § 160.103 of HIPAA.
Covered Entity: the meaning given in 45 CFR § 160.103 of HIPAA.
Disclosure: the release, transfer, provision of access to, or divulging in a manner of information outside the entity holding the information, and **Disclose** shall be interpreted accordingly.
HIPAA: the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 as amended, by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations.
HIPAA Privacy Rule: the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164.
PHI: Protected Health Information as defined in 45 CFR § 160.103, provided that it is limited to such Protected Health Information that is actually received by KnowBe4 from, or created, received, maintained, or transmitted by KnowBe4 on Customer's behalf through Customer's use of the Services.
Unsuccessful Security Incident: an attempt to gain access Customer PHI or the infrastructure and networks that provide the Services (including denial of service attacks, pings, attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, packet sniffing or other unauthorized access to traffic data) that does not result in unauthorized access to Customer PHI.

2. BACKGROUND

2.1. As part of Customer's use of the Services, Customer may transfer, store, share, host or Disclose to KnowBe4certain information which may constitute PHI.
2.2. In KnowBe4's role as provider of the Services to you, KnowBe4 may at times perform the role of a Business Associate.
2.3. Both parties have entered into this BAA in order to ensure that where KnowBe4 acts as a Business Associate on Customer's behalf, the privacy and security of Customer PHI is protected in compliance with the HIPAA Privacy Rule.
2.4. Affiliates and Users. If Customer is an organisation with more than one Affiliate company or User, Customer acknowledges it is responsible for its own compliance and that of Customer's Affiliate companies' and Users with this BAA.

3. OUR RESPONSIBILITIES AND PERMITTED USE

3.1. Performance of the Agreement. To the extent that KnowBe4 acts as a Business Associate on Customer's behalf then, subject to the terms of this BAA, KnowBe4, KnowBe4's Affiliates and relevant sub-contractor business associates may Use or Disclose PHI for or on behalf of Customer in order to perform KnowBe4's obligations under this BAA and/or the Agreement (provided that such Use or Disclosure would not violate HIPAA if done by Customer). In such circumstances KnowBe4 agrees to: (a) not Use or Disclose PHI other than as permitted or required by the Agreement, this BAA, or as required by law or agreed to by Customer; and (b) use reasonable and appropriate safeguards and comply with 45 CFR Part 164 Subpart C with respect to electronic PHI, to prevent Use or Disclosure of PHI other than as provided for in this BAA. KnowBe4 may also use and disclose PHI for KnowBe4's proper management and administration or to carry out KnowBe4's legal responsibilities, provided that if PHI is disclosed, such disclosure is required by law, or KnowBe4 obtains reasonable assurance from the person to whom the PHI is disclosed that the PHI will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person or entity, and the person or entity agrees to notify KnowBe4 of any instances in which the confidentiality of the PHI has been compromised of which it becomes aware.
3.2. Customer acknowledges and agrees that the provision by KnowBe4 of the Services to Customer, does not constitute a prohibited Use or Disclosure under 45 CFR § 164.502(a)(5)(i), and Customer has obtained any and all necessary consents, authorizations or permissions required by applicable law for KnowBe4 to provide the Services.
3.3. Reporting. To the extent that KnowBe4 acts as a Business Associate on Customer's behalf, KnowBe4 agrees to report to Customer any: (a) Use or Disclosure of PHI not permitted or required by this BAA or the Agreement of which KnowBe4 becomes aware; (b) breaches of unsecured PHI of which KnowBe4 becomes aware as required at 45 CFR 164.410; and (c) security incidents of which KnowBe4 becomes aware (provided that notice is hereby deemed given in respect of Unsuccessful Security Incidents and no further notice of such incidents shall be required or given). Notifications in this Section will be made by KnowBe4 without unreasonable delay. Any notification or response to a breach is not, and will not be construed as, acknowledgement by KnowBe4 or any relevant sub-contractor business associate of any fault or liability in respect to it.

3.4. Sub-contractor Business Associates. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), KnowBe4 will require that relevant sub-contractor business associates who maintain, store or transmit Customer's PHI on behalf of KnowBe4 pursuant to this BAA: (a) agree to substantially similar restrictions and conditions that apply to KnowBe4 with respect to such PHI; and (b) use reasonable and appropriate safeguards and comply with 45 CFR Part 164 Subpart C with respect to electronic PHI, to prevent Use or Disclosure of PHI other than as provided for in this BAA.

3.5. Disclosure to the Secretary. KnowBe4 agrees to make KnowBe4's internal practices, books, and records relating to the PHI that KnowBe4 receives from Customer available to the Secretary of the US Department of Health and Human Services for purposes of determining Customer's compliance with the HIPAA Privacy Rule (subject to attorney-client and other applicable legal privileges).

3.6. No Marketing. KnowBe4 shall not use PHI for Marketing and shall not violate the HIPAA prohibition on the sale of PHI.

4. AVAILABILITY OF PHI

4.1. Limited Access. Customer acknowledges and agrees that since the nature of the Services that KnowBe4 provides to Customer does not consist of regular access or management of PHI by KnowBe4 or sub-contractor business associates: (a) KnowBe4 may not be able to make available PHI to the extent and in the manner required by 45 CFR § 164.524; (b) KnowBe4 cannot make PHI available for amendment or incorporate any amendments to PHI in accordance with the requirements of 45 CFR § 164.526; and (c) KnowBe4 cannot make PHI available for purposes of accounting of Disclosures, as required by 45 CFR § 164.528. Customer expressly acknowledges that these requirements shall be Customer's sole responsibility.

4.2. Restrictions on Disclosures. KnowBe4 agrees to comply with any requests for restrictions on certain Disclosures of PHI pursuant to 45 CFR § 164.522 which Customer has agreed to and which Customer notifies KnowBe4 in writing. Customer agrees that the provision of the Services (including the encryption, transmission, or de-encryption of Customer Data and PHI) will not breach the terms of this Section 4.2 and that compliance with any restrictions on Disclosures of PHI shall be the sole responsibility of Customer and the entities and individuals to, and with, whom Customer exchanges PHI.

5. YOUR OBLIGATIONS

5.1. Customer is responsible for Customer's compliance with HIPAA including appropriate privacy and security safeguards to protect PHI.

5.2. YOU MUST NOT INCLUDE PHI IN ANY REQUESTS THAT YOU MAKE TO US THROUGH SUPPORT.

5.3. Customer will not ask KnowBe4 or any relevant Sub-Processor to Use or Disclose PHI in any manner that would not be permitted under HIPAA if done by a Covered Entity (unless permitted for a Business Associate under HIPAA).

6. EXCLUSIONS

6.1. KnowBe4 does not act as, and will not have the responsibilities or obligations of, a Business Associate, once the PHI is sent from the Services over the Internet as directed by Customer.

7. TERM AND TERMINATION

7.1. Term. This BAA comes into force on the date Customer signs it and shall continue in full force until the earlier of: (a) termination in accordance with this Section 7; (b) termination or expiry of the Agreement; or (c) KnowBe4 ceasing to act as a Business Associate on Customer's behalf in the provision of the Services.

7.2. Termination for Cause. A party to this BAA may terminate it: (a) immediately by notice to the other if the other is in material breach of this BAA which is not remediable; (b) through 30 days written notice to the other of a material breach if that breach remains unremedied at the expiry of that period.

7.3. Effects of Termination or Expiration. Following termination or expiration of this BAA, KnowBe4 will securely return or destroy all PHI in Customer's accounts to the fullest extent technically possible in the circumstances and will have no obligation to store it and no liability to Customer for its destruction and disposal. If such return or destruction is not feasible, then KnowBe4 will extend the protections of this BAA to the relevant PHI and limit further Uses and Disclosures to those purposes that make the return or destruction of the information not feasible. In addition, the other consequences of termination set out in the Agreement shall apply where the Agreement is also terminating or expiring.

8. GENERAL

8.1. Notices. Customer agrees that any reports, notifications or other notices by KnowBe4 under this BAA may be sent to Customer electronically. Customer must provide KnowBe4 with appropriate information (including contact name, title, role, email address, contact telephone number, and the name of the organization(s) for which the contact is responsible). Customer will ensure that this information remains up-to-date while this BAA is in force. Failure to do so may delay or inhibit KnowBe4's ability to provide Customer with information and notifications.

8.2. Third-Party Rights. There are no third-party beneficiaries under this BAA.

8.3. Interpretation.This BAA and/or the Agreement shall be interpreted as broadly as necessary to implement and comply with the mandatory provisions of HIPAA. The parties agree that this BAA shall be interpreted in favor of their intent to comply with HIPAA and the HIPAA Regulations and therefore any ambiguity shall be resolved in favor of a meaning that complies and is consistent with those laws. In this BAA: (a) the terms *including*, *includes* or any similar expression shall be construed as illustrative and will not limit the scope of words that follow them; (b) references to *writing* or *written* includes email (except that email cannot be used for serving notices connected to legal proceedings); and (c) any obligation on a party not to do something includes an obligation not to allow that thing to be done.

8.4. No Change to the MSA. Except where this BAA conflicts with the Agreement in which case the terms of this BAA shall control solely with respect to the subject matter herein, all other provisions of the Agreement remain unchanged.

8.5. Amendments and Variations. Amendments to this BAA may not be made orally. No amendment or variation of, or to, this BAA shall be effective unless it is in writing and signed by both Customer and KnowBe4 (or their respective authorized representatives). This Section shall not apply to any document or information referred to at a URL within the terms of this BAA which may be updated from time to time by KnowBe4.

8.6. Liability. KnowBe4's liability under or in connection with this BAA is subject to the limitations on liability contained in the Agreement.

8.7. Ownership of PHI. As between Customer and KnowBe4, any PHI transferred, stored, shared, hosted or otherwise Disclosed under the terms of this BAA shall be deemed to be Customer's and Customer's Affiliates' (as applicable) exclusive property. In no event will KnowBe4 claim any rights with respect to it.

8.8. Governing Law and Jurisdiction. This BAA shall be governed by and interpreted in accordance with the laws set out in the Agreement, and the courts set out in the Agreement shall have exclusive jurisdiction over any claims, disputes, actions or proceedings arising under or in relation to this BAA.