***Note to copy:***

*For Enterprise Customers that would like to receive a pdf copy of the HubSpot Business Associate Agreement (BAA), we have made this copy available to you for your convenience. The HubSpot BAA is included in the HubSpot Sensitive Data Terms available at https://legal.hubspot.com/sensitive-data-terms as Annex I.*

*No changes made to this copy are agreed to by HubSpot, Inc. or its Affiliates.*

*Please note that we update the HubSpot Sensitive Data Terms as we describe in the 'Changes to Sensitive Data Terms' section below. If you would like to receive an email notification when we update the HubSpot Terms of Service, please complete the form found at https://legal.hubspot.com/subscribe-tos-updates.*

*If you have any questions, please contact your HubSpot representative.*

# HUBSPOT BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is made part of the agreement between HubSpot, Inc. ("Business Associate" or "HubSpot") and Customer for the use of the applicable HubSpot Services to which Customer has subscribed to in an Order Form, Statement of Work, or other agreement with HubSpot (the "Agreement"). Business Associate and Customer may be referred to herein as a "Party" and together as the "Parties."

RECITALS:

(A) Customer is a "covered entity" or "business associate" as such terms are defined under HIPAA and as such is required to comply with the requirements thereof regarding the confidentiality and privacy of Protected Health Information.

(B) In connection with the provision of HubSpot Services to Customer, the parties anticipate that HubSpot may receive Protected Health Information for or on behalf of Customer.

(C) By providing services pursuant to the Agreement and creating and/or receiving Protected Health Information for or on behalf of Customer, Business Associate will become a business associate or subcontractor of Customer, as such terms are defined under HIPAA, and will therefore have obligations regarding the confidentiality and privacy of Protected Health Information that Business Associate creates for, or receives from or on behalf of, Customer.

(D) This BAA applies only to the extent Customer is a "covered entity" or "business associate" as those terms are defined by HIPAA where Customer is sharing Protected Health Information with HubSpot.

1. Definitions.

For the purposes of this BAA, capitalized terms will have the meanings ascribed to them below. All capitalized terms used but not otherwise defined herein will have the meaning ascribed to them by HIPAA.

a. “HIPAA” means, collectively, the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations (referred to herein as the “HIPAA Rules”), including the Privacy Rule, the Breach Notification Rule, the Security Rule and the Enforcement Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health (HITECH) Act and by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act: Other modifications to the HIPAA Rules; Final Rule (commonly referred to as the Omnibus Final Rule).

b. “HubSpot Services” means the HubSpot services Customer has subscribed to in an Order Form, Statement of Work, or other written agreement in which HubSpot has explicitly authorised for use by Customer to process PHI.

c. “Protected Health Information” or “PHI” has the same meaning as the term “protected health information” or “electronic protected health information,” respectively, in 45 CFR § 160.103; provided that, for purposes of this BAA, such term is limited to protected health information that is received and maintained by HubSpot from or on behalf of Customer through the HubSpot Services.

d. “Secretary” will refer to the Secretary of the U.S. Department of Health and Human Services.

e. “Unsecured PHI” will mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary (e.g., encryption). This definition applies to both hard copy PHI and electronic PHI.

f. “Unsuccessful Security Incidents” means, without limitation, pings and other broadcast attacks on HubSpot’s firewall, port scans, unsuccessful log-on attempts, denial of service attacks, as long as no such incident results in unauthorised access, acquisition, Use, or Disclosure of PHI.

2. Business Associate’s Obligations.

a. Use and Disclosure of PHI.

i. Business Associate warrants that it, its agents and its subcontractors: (i) will use or disclose PHI only in connection with fulfilling its rights, duties and obligations under this BAA and the Agreement; (ii) will not use or disclose PHI other than as permitted or required by this BAA and the Agreement or required by law; (iii) will not use or disclose PHI in any manner that violates applicable federal and state laws or would violate such laws if used or disclosed in such manner by Customer; and (iv) will only use and disclose the minimum necessary PHI for its specific purposes. Customer agrees that Business Associate may rely on Customer’s instructions to determine if uses and disclosures meet this minimum necessary requirement.

ii. Subject to the restrictions set forth throughout this BAA, Business Associate may use the information received from Customer if necessary for (i) the proper management and administration of Business Associate; or (ii) to carry out the legal right and responsibilities of Business Associate.

iii. Subject to the restrictions set forth in this BAA, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that (1) disclosures are required by law; or (2) Business Associate obtains reasonable assurances from the person or entity to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes permitted under the Agreement to the person or entity, and the person or entity notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. Business Associate will comply, where applicable, with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI to prevent use or disclosure of such electronic PHI other than as provided for by this BAA or the Agreement.

iv. Business Associate is permitted, for Data Aggregation purposes to the extent permitted under HIPAA, to use, disclose, and combine PHI created or received on behalf of Customer by Business Associate pursuant to this BAA with PHI, as defined by 45 C.F.R. 160.103, received by Business Associate in its capacity as a business associate of other covered entities, to permit data analyses that relate to the Health Care Operations of the respective covered entities and/or Customer.

v. Business Associate may de-identify to a HIPAA standard any and all PHI created or received by Business Associate under this BAA. Once PHI has been de-identified pursuant to 45 CFR 164.514(b), such information is no longer Protected Health Information and no longer subject to this BAA.

b. Safeguards. Business Associate will employ appropriate administrative, technical and physical safeguards to protect the confidentiality of PHI and to prevent the use or disclosure of PHI in any manner inconsistent with the terms of this BAA or the Agreement. Business Associate will comply, where applicable, with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI to prevent use or disclosure of such electronic PHI other than as provided for by this BAA or the Agreement.

c. Audits and Records. Business Associate will, in accordance with HIPAA, make available to the Secretary Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Customer for purposes of determining Customer's compliance with its obligations under HIPAA.

d. Individuals' Rights to Their PHI.

i. To the extent Business Associate maintains PHI in a Designated Record Set, in order to allow Customer to respond to a request by an Individual for access to PHI pursuant to 45 CFR Section 164.524, Business Associate, within ten (10) business days upon receipt of written request by Customer, will make available to Customer such PHI.

1. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate will forward such request to Customer within five (5) business days.

2. Customer will be responsible for making all determinations regarding the grant or denial of an Individual's request for PHI and Business Associate will make no such determinations. Except as required by law, only Customer will be responsible for releasing PHI to an Individual pursuant to such a request. Any denial of access to PHI determined by Customer pursuant to 45 CFR

Section 164.524, and conveyed to Business Associate by Customer, will be the responsibility of Customer, including resolution or reporting of all appeals and/or complaints arising from denials.

ii. To the extent Business Associate maintains PHI in a Designated Record Set, in order to allow Customer to respond to a request by an Individual for an amendment to PHI, Business Associate will, within ten (10) business days upon receipt of a written request by Customer, make available to Customer such PHI:

1. In the event that any Individual requests amendment of PHI directly from Business Associate, Business Associate will forward such request to Customer within five (5) business days.

2. Customer will be responsible for making all determinations regarding the grant or denial of an Individual's request for an amendment to PHI and Business Associate will make no such determinations. Any denial of amendment to PHI determined by Customer pursuant to 45 CFR Section 164.526, and conveyed to Business Associate by Customer, will be the responsibility of Customer, including resolution or reporting of all appeals and/or complaints arising from denials.

3. Within ten (10) business days of receipt of a request from Customer to amend an individual's PHI in the Designated Record Set, Business Associate will incorporate, or make available PHI for Customer to incorporate, any approved amendments, statements of disagreement, and/or rebuttals into its Designated Record Set as required by 45 CFR Section 164.526.

iii. In order to allow Customer to respond to a request by an Individual for an accounting pursuant to 45 CFR Section 164.528, Business Associate will, within ten (10) business days of a written request by Customer for an accounting of disclosures of PHI about an Individual, make available to Customer such PHI. Business Associate will provide Customer with the following information: (1) the date of the disclosure; (2) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (3) a brief description of the PHI disclosed; and (4) a brief statement of the purpose of such disclosure.

1. In the event that any Individual requests an accounting of disclosures of PHI directly from Business Associate, Business Associate will forward such request to Customer within five (5) business days.

2. Customer will be responsible for preparing and delivering an accounting to Individual.

3. Business Associate will implement an appropriate record keeping process to enable it to comply with the requirements of this BAA.

e. Disclosure to Third Parties. Business Associate will obtain and maintain a written agreement with each subcontractor or agent that has or will have access to PHI, which is received from, or created or received by, Business Associate for or on behalf of Customer, pursuant to which agreement such subcontractor and agent agrees to be bound by the same standards of restrictions, terms, and conditions that apply to Business Associate pursuant to this Agreement with respect to such PHI.

f. Reporting Obligations.

i. Business Associate will report any Breach to Customer no later than ten (10) business days after discovery by Business Associate. Notice of a Breach will include, to the extent such information is available: (1) the identification of each individual whose PHI has been, or is

reasonably believed to have been, accessed, acquired, or disclosed during the Security Breach; (2) the date of the Breach, if known, and the date of discovery of the Breach; (3) the scope of the Breach; and (4) the Business Associate's response to the Breach.

ii. In the event of a use or disclosure of PHI that is improper under this BAA but does not constitute a Breach, Business Associate will report such use or disclosure to Customer within ten (10) business days after the date on which Business Associate becomes aware of such use or disclosure.

iii. The parties acknowledge that Unsuccessful Security Incidents occur within the normal course of business and the parties stipulate and agree that this paragraph constitutes notice by Business Associate to Customer for such unsuccessful Unsuccessful Security Incidents.

3. Customer Obligations.

a. Permissible Requests.

i. Customer will not request Business Associate to use or disclose PHI in any manner that would violate applicable federal and state laws if such use or disclosure were made by Customer.

ii. Customer will be compliant with all applicable laws and regulations pertaining to PHI Customer sends, or directs to be sent, to Business Associate.

b. Notifications.

i. Customer will notify Business Associate of any limitation in any applicable notice of privacy practices in accordance with 45 CFR Section 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

ii. Customer will notify Business Associate of any changes in, or revocation of, permission by individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

iii. Customer will notify Business Associate of any restriction to the use or disclosure of PHI that Customer has agreed to in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

4. Term and Termination.

a. Material Breach. Where either Party has knowledge of a material breach by the other Party, the non-breaching Party will provide the breaching Party with an opportunity to cure. Where said breach is not cured to the reasonable satisfaction of the non-breaching Party within twenty (20) business days of the breaching Party's receipt of notice from the non-breaching Party of said breach, the non-breaching Party will, if feasible, terminate this BAA and the portion(s) of the Agreement affected by the breach. Where either Party has knowledge of a material breach by the other Party and cure is not possible, the non-breaching Party will, if feasible, terminate this BAA and the portion(s) of the Agreement affected by the breach.

b. Return or Destruction of PHI. Upon termination of this BAA for any reason, Business Associate will:

i. If feasible as determined by Business Associate, return or destroy all PHI received from, or created or received by Business Associate for or on behalf of Customer that Business Associate or any of its subcontractors and agents still maintain in any form, and Business Associate will retain no copies of such information; or

ii. If Business Associate determines that such return or destruction is not feasible, extend the protections of this BAA to such information and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible, in which case Business Associate's obligations under this Section 4(b) will survive the termination of this BAA.

5. General.

a. Amendment. If any of the regulations promulgated under HIPAA are amended or interpreted in a manner that renders this BAA inconsistent therewith, the Parties will cooperate in good faith to amend this BAA to the extent necessary to comply with such amendments or interpretations.

b. Interpretation. Any ambiguity in this BAA will be resolved to permit the Parties to comply with HIPAA.

c. Indemnification and Limitation of Liability. The parties agree and acknowledge that the indemnification obligations and limitation of liability provisions contained under the Agreement will apply and govern each party's performance under this BAA.

d. Conflict; Order of Precedence. In the event that any terms of this BAA conflict with any terms of the Agreement, the terms of this BAA will govern and control over the conflicting term in the Agreement. All other nonconflicting terms of the Agreement will remain valid and enforceable.