Brandwatch Business Associate Addendum – Last updated: 4 June 2025

This Business Associate Addendum ("BAA") supplements the Service Appendix entered into between the parties identified on the Order as "Supplier" and "Customer". Capitalized terms used but not defined in this BAA shall have the meanings set forth in the master agreement agreed to between the parties ("Master Agreement"), unless otherwise defined in this BAA.

WHEREAS, Customer is a Covered Entity or a Business Associate of a Covered Entity under the Health Insurance Portability and Accountability Act of 1996 and its regulations, as amended by the Health Information Technology for Economic and Clinical Health Act ("HIPAA" and "HITECH," respectively), and in the provision of the Services to Customer, Supplier may incidentally or inadvertently receive, or maintain, Protected Health Information ("PHI") on behalf of Customer;

WHEREAS, Supplier provides a cloud-based social media management platform which is not designed to be HIPAA-compliant and is not intended to receive, store, or process Protected Health Information, and this BAA prohibits Customer from purposefully including PHI or other sensitive personal data in Customer Data submitted to the Services;

1. Definitions

For purposes of this BAA, the following terms have the meaning set forth below. Capitalized terms not defined in this BAA have the meanings given in the Master Agreement or under HIPAA or the HIPAA Rules, as applicable:

- **"Protected Health Information"** or **"PHI"** shall have the same meaning as the term "protected health information" in 45 C.F.R. §160.103, and is limited to the information, received, or maintained, by Supplier from or on behalf of Customer through the Services. PHI does not include information that is de-identified in accordance with 45 C.F.R. §164.514.

- **"Covered Entity"** shall have the meaning given in 45 C.F.R. §160.103. In this BAA, Customer is the Covered Entity (or a Business Associate acting on behalf of a Covered Entity) that has engaged Supplier to perform services.

- **"Business Associate"** shall have the meaning given in 45 C.F.R. §160.103.

- **"HIPAA Rules"** means collectively the Privacy, Security, Breach Notification, and Enforcement Rules promulgated under HIPAA and HITECH (45 C.F.R. Parts 160 and 164).

- **"Customer Data"** means data that Customer makes available to Supplier for the purpose of Supplier processing that data on Customer's behalf.

- **"Privacy Rule"** means the Standards for Privacy of Individually Identifiable Health Information" promulgated under HIPAA and codified in 45 C.F.R. Parts 160 and 164, Subparts A and E.

- **"Supplier Data"** means any data in Supplier's platform that Supplier uses in providing the Services, excluding Customer Data.

- **"Services"** means the cloud-based social media management software-as-a-service and related services provided by Supplier to Customer under the Master Agreement.

2. Scope and Applicability

2.1. **Limited Applicability of BAA.** The Parties agree that this BAA only applies to the extent that Supplier is acting as a "Business Associate" of Customer as defined by HIPAA – namely, solely in the event and to the extent Supplier *acts in a way to establish a Business Associate relationship with*

Customer in the event Supplier inadvertently receives or has access to any PHI in the course of providing the Services. This BAA shall not apply to usage of the Services that does not involve any PHI or to any Supplier Data that might include PHI. Customer acknowledges and agrees that the Services are not intended to be used for PHI, and Customer shall not deliberately upload, transmit, or store PHI as part of Customer Data. Nothing in this BAA shall be construed to obligate Supplier to receive or process PHI, or to make the Services compliant with HIPAA, beyond the specific commitments set forth herein for handling inadvertently received PHI.

2.2. **Infrastructure Limitations; No Intended PHI Use.** Customer understands that the Services do not include integration with or access to any Customer electronic health record systems or internal networks, and operate by interfacing with third-party social media platforms (e.g. Meta, X, etc.) which themselves are not HIPAA-compliant environments. Because of these inherent limitations, the parties agree that social media is not an appropriate channel for transmitting PHI and Customer shall not intentionally use the Services to collect or manage PHI.

2.3. **Third-Party Services Disclaimer.** Customer acknowledges that the Services involve interactions with social network platforms and other integrated services which may not comply with HIPAA, HITECH, or the HIPAA Rules ("Third-Party Services"). Supplier makes no representation or warranty that any such Third-Party Services are HIPAA compliant. Supplier disclaims all liability for the privacy or security of PHI handled by or passing through any Third-Party Services.

3. Permitted Uses and Disclosures by Supplier

3.1. **Permitted Use for Services.** Except as otherwise limited in this BAA, Supplier is permitted to use and disclose PHI solely for the purpose of providing the Services to Customer in accordance with the Master Agreement. Supplier may disclose PHI as required by Law.

3.2. **Management and Administration.** Notwithstanding any other provision of this BAA, Supplier is permitted to use and disclose PHI for Supplier's proper management and administrative purposes or to carry out Supplier's legal responsibilities, provided that any disclosure for such purposes: (a) is required by Applicable Law; or (b) is made to a subcontractor or other third party for the purpose of assisting Supplier with its administrative or legal requirements, and in the latter case Supplier shall obtain reasonable assurances from the recipient that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed, and that the recipient will notify Supplier of any instance of which it becomes aware in which the confidentiality of the PHI has been breached.

3.3. **De-Identification and Aggregation.** Supplier may de-identify or aggregate any PHI it may inadvertently receive, in accordance with 45 C.F.R. §164.514(b), and use or disclose such de-identified data freely (for example, to analyze interactions for product improvement or compile aggregated statistics), provided that no such use or disclosure violates the applicable HIPAA Rules. Supplier may also combine PHI with other data to perform data aggregation services (as defined by 45 C.F.R. §164.504(e)(2)(i)(B)) relating to Customer's health care operations, *only* to the extent such aggregation is needed to carry out the Services and permitted by law.

4. Supplier's Privacy and Security Obligations

In the event Supplier inadvertently receives or has access to any PHI in the course of providing the Services, Supplier agrees to comply with the following obligations :

- **4.1 Safeguards.** Supplier shall implement and maintain appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any PHI that Supplier collects, receives, maintains, or transmits on behalf of Customer. Supplier will use commercially reasonable measures (including encryption of data at rest and in transit, access controls, and personnel training) to prevent any use or disclosure of PHI other than as permitted by this BAA or required by Applicable Law.

- **4.2 Privacy Rule Compliance.** To the extent that Supplier carries out any obligation of Customer under the Privacy Rule, Supplier shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.

5. Customer's Obligations and Risk Mitigation Responsibilities

Customer, as a Covered Entity (or as a Business Associate of a Covered Entity, as the case may be), acknowledges and agrees to the following obligations, to facilitate compliance with HIPAA and to minimize the risk of any PHI being transmitted via the Services:

- **5.1 No Impermissible Use of Services for PHI.** Customer shall not request or require Supplier to use or disclose PHI in any way that would not be permissible under the HIPAA Rules if done by Customer directly. Customer shall not intentionally transmit, upload, or store any PHI (except for de-identified data) in the Services, and shall not otherwise use the Services to further any treatment, payment, or healthcare operations involving PHI. The parties agree that any PHI that does enter the Services will be only that which is inadvertently or uncontrollably submitted by individuals on social media. Customer remains responsible for ensuring its own use of the Services complies with HIPAA and for preventing any avoidable disclosures of PHI via social media.

- **5.2 Implementation of Preventive Measures.** Customer will use reasonable efforts to configure and utilize the Services in a manner that discourages or prevents the sharing of PHI. Without limiting the foregoing, Customer will make use of available features and best practices to reduce the risk of receiving PHI through social media. Such measures include, but are not limited to, the following:

    5.2.1 Message Disclaimers (Customer Only): Posting clear disclaimers on Customer's social media inbox (and enabling any available automated disclaimer or greeting for direct messages) to notify users that Customer cannot receive personal health information via social media.

    5.2.2 Automated Responses and Redirects (Customer Only): For example, if a user attempts to discuss symptoms or requests medical advice via a direct message, an automated reply can be triggered to inform them that the channel is not secure for such discussions and provide an alternative contact (such as a phone number or patient portal link) for handling medical inquiries.

    5.2.3 PHI Tagging Tools (Customer; with Supplier Tooling): Utilizing any filtering tools provided as part of the Services to flag and delete messages or posts that appear to contain PHI. Customer shall review items labeled as PHI without undue delay and, where appropriate, delete the content from the Services. If Customer cannot delete an item through user interface, Customer may email socialsupport@brandwatch.com for requesting permanent deletion.

5.3 Consents and Authorizations. Customer represents and warrants that it has obtained any consents, authorizations, or other permissions that may be required by law (including HIPAA) for Supplier to receive and process PHI in the manner contemplated by this BAA. To the extent any individual's authorization is needed for Supplier to perform the Services involving that individual's PHI, Customer shall ensure such authorization is in place before that PHI is introduced into the Services. Customer shall not provide Supplier with any PHI that is not lawfully obtained or that Customer would be prohibited from disclosing to a Business Associate under Applicable Law.

5.4 Compliance with HIPAA. Customer shall not violate HIPAA through its use of the Services and shall not cause Supplier to be out of compliance with HIPAA by its acts or omissions. Customer remains responsible for its own HIPAA compliance obligations (such as providing breach notifications to

individuals, if a breach of PHI originated from Customer's actions, or ensuring appropriate notices and disclosures to patients about the use of service providers like Supplier). Customer shall cooperate with Supplier in good faith to address any incident or compliance inquiry related to PHI in the Services, including assisting Supplier in responding to any governmental or regulatory investigations or requests (as needed and applicable to Customer).

6. Term and Termination

6.1. **Term.** This BAA shall become effective when it is signed by the parties and it continues until all Orders have expired or been terminated in accordance with the terms of this BAA.

6.2. **Deletion of PHI.** Upon termination or expiration of this BAA (or the Master Agreement) for any reason, Supplier shall delete all PHI received from Customer unless required to retain the PHI under Applicable Law.

6.3. **Effect of Termination on Services.** No termination of this BAA shall be construed to waive or modify any terms of the Master Agreement unrelated to PHI. However, if the Master Agreement is terminated for any reason, this BAA shall automatically terminate concurrently, except that all provisions regarding the protection of PHI shall survive to the extent Supplier continues to possess any PHI after termination.

7. Miscellaneous

7.1. **Regulatory Amendment.** The Parties acknowledge that federal or state laws relating to electronic health information privacy may be amended over time, and that additional regulations or guidance may be issued by the Department of Health and Human Services. In the event any change in law or regulation materially alters the obligations of either party under this BAA, the Parties agree to negotiate in good faith to amend this BAA as needed to ensure continued compliance with the applicable law. If the Parties are unable to agree on an amendment within a reasonable time, either party may terminate this BAA and the Master Agreement upon written notice, if required to avoid a violation of law.

7.2 Governing Law. The governing law of the Master Agreement applies to this BAA.