

## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“**BAA**”) forms part of our Terms of Service (“**Agreement**”) whether you are an existing customer who accepted the Agreement or a new customer accepting the Agreement now. You acknowledge that you, on your own behalf as an individual and on behalf of your employer or another legal entity (collectively, “**Covered Entity**” “**you**”, “**your**” or the “**Customer**”) have read and understood and agree to comply with this BAA, and are entering into a binding legal agreement with monday.com Ltd the owner of monday.com (“**monday.com**”, “**us**”, “**we**”, “**our**” or “**service provider**”) to reflect the parties’ agreement with regard to the Business Associate uses and/or disclosures of the Covered Entity’s Protected Health Information defined at 45 C.F.R. § 160.103 (“**PHI**”, which, for the terms of this Agreement, collectively pertains to PHI in any medium, whether electronic, paper or verbal).

Both parties shall be referred to as the “**Parties**” and each, a “**Party**”. Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement or under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as may be updated from time to time (collectively, “**HIPAA**”). You represent and warrant that you have, or you were granted, full authority to bind the Customer to this BAA. If you cannot, or do not agree to, comply with, and be bound by, this BAA or do not have authority to bind the Customer or any other entity, please do not supply or provide PHI to us. You enter into this BAA on behalf of yourself and, to the extent required under HIPAA and applicable data protection laws and regulations, in the name and on behalf of the Customer and the Customer’s affiliates, if and to the extent that you or the Customer processes PHI for which such affiliates qualify as a “**Covered Entity**”. For the purposes of this BAA only, and except where indicated otherwise, the term “**Covered Entity**” shall include yourself, the Customer and/or the Customer’s affiliates.

In the course of providing the Services pursuant to the Agreement, we may access, use, disclosure, and/or process PHI on your and/or Customer’s behalf, in the capacity of a “Business Associate”. The Parties agree to comply with the following provisions with respect to any PHI, each acting reasonably and in good faith. If you need a signed copy of this BAA, you can download this BAA at [www.monday.com/terms/hipaa-baa](http://www.monday.com/terms/hipaa-baa), send a signed copy to [legal@monday.com](mailto:legal@monday.com) and we’ll provide you a countersigned copy. In the event of any conflict between certain provisions of this BAA and the provisions of the Agreement, the provisions of this BAA shall prevail over the conflicting provisions of the Agreement.

The Business Associate currently uses and/or discloses Covered Entity’s PHI in order to provide the Services, as further outlined in the Agreement between the Parties; and by providing Services pursuant to the Agreement, Business Associate shall become a business associate of Covered Entity, as such term is defined under HIPAA, and will therefore have obligations regarding the confidentiality and privacy of PHI that Business Associate creates for, or receives from or on behalf of, Customer.

1. **Permitted Uses and Disclosures.** The Business Associate may use and disclose PHI necessary to perform its obligations to the Covered Entity as set out in the Agreement or as otherwise permitted or required by law under HIPAA, provided that Business Associate shall not use or disclose PHI in a manner that would not be permitted if done by Covered Entity. The Business Associate may also:
  - (a) use PHI (i) as necessary for its proper management and administration, or (ii) to carry out its legal responsibilities;

- (b) disclose PHI to third parties for the same purposes so long as (i) the disclosure is required by law or (ii) the Business Associate obtains satisfactory assurances from said third party 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 third party will notify the Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached; and
- (c) Business Associate agrees to make uses and disclosures and requests for PHI consistent with Covered Entity's minimum necessary policies and procedures.

## 2. Obligations of the Business Associate.

- (a) Limitation on Disclosure. The Business Associate agrees not to use or further disclose PHI other than as permitted or required herein, in any written Agreement (including the Agreement), or as required by law.
- (b) Safeguards. The Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, stores, maintains or transmits on behalf of the Covered Entity pursuant to this Agreement or any relevant agreement, and shall prevent the use or disclosure of Covered Entity's PHI other than as provided for in this Agreement or as required by law.
- (c) Reporting of Uses/Disclosures Not Provided for in Agreement. The Business Associate agrees to report to the Covered Entity any use or disclosure of PHI not provided for herein or by any written agreement of which it becomes aware.
- (d) Mitigation. The Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
- (e) Use of Agents/Subcontractors. The Business Associate agrees to ensure that any agents, including a subcontractor, to whom the Business Associate provides PHI received from, or created or received by, Business Associate on behalf of the Covered Entity, agree to substantially similar restrictions and conditions that apply to the Business Associate with respect to PHI. The Business Associate, pursuant to its obligations under HIPAA and this Agreement, is fully responsible for ensuring that it enters into an agreement with its subcontractors containing obligations no less restrictive than the terms of this Agreement.
- (f) Access to PHI. Within fifteen (15) days of receiving a written request from the Covered Entity for a copy of PHI, the Business Associate agrees to make the requested PHI available to the Covered Entity to enable the Covered Entity to respond to an individual who seeks to inspect or copy PHI, unless the Business Associate considers that there are reasonable grounds for the denial of such request in accordance with 45 C.F.R. § 164.524, in which case it shall notify the Covered Entity accordingly. Business Associate is required to comply with the Security Rule with regard to electronic PHI, including but not limited to, making available upon written request, copies of PHI in electronic format, when PHI is stored electronically.
- (g) Amendment of PHI. Within fifteen (15) days of receiving a written request from the Covered Entity to make an amendment to the PHI, the Business Associate will make such amendment and will inform any holder of the PHI that is known to the Business Associate

that an amendment has been made, unless the Business Associate considers that there are reasonable grounds for the denial of such request in accordance with 45 C.F.R. § 164.526, in which case it shall notify the Covered Entity accordingly.

- (h) Accounting of Certain Disclosures. Within thirty (30) days of receiving a written request from the Covered Entity for an accounting of disclosures of PHI about an individual, the Business Associate shall provide to the Covered Entity a listing of the persons or entities to which the Business Associate has disclosed PHI about the individual within the prior six (6) years, along with the dates of, reasons for, and brief descriptions of the disclosures to enable the Covered Entity to respond to an individual seeking an accounting of the disclosures of the individual's PHI. (See 45 C.F.R. § 164.528.)
- (i) Access to Books and Records. The Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, created by, or received by the Business Associate on behalf of the Covered Entity available upon request to the U.S. Department of Health and Human Services so that it may evaluate the Covered Entity's compliance with the Privacy Rule.
- (j) Obligations of Business Associate Upon Termination. The Business Associate shall, at the termination of any agreement, or of the uses and/or disclosures of the PHI by the Business Associate, if feasible, return or allow the Covered Entity to destroy all PHI received from, created by, or received by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form in connection with this Agreement through a deletion option provided by the Business Associate and retain no copies of such information or, if such return or destruction is not feasible extend the protections of this Agreement to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.
- (k) Reporting of Security Incident. The Business Associate shall report to the Covered Entity any Security Incident of which it becomes aware. (Under 45 C.F.R. § 164.304, a Security Incident is defined as the attempted or successful unauthorized access, use, disclosure, or destruction of information or interference with system operations in an information system.) Notwithstanding the foregoing, the Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents. Unsuccessful Security Incidents shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, or through any other mechanism so long as no such incident results in Unauthorized access, use or disclosure of PHI.

### 3. Breach Notification Procedures.

- (a) Reporting of Uses/Disclosures Not Provided for in Agreement. Business Associate agrees to report to Covered Entity any Breach – including, without limitation any alleged unauthorized, impermissible acquisition, access, uses or disclosures of PHI (in any form) – in full compliance with HIPAA. Such notification of any alleged unauthorized uses or disclosures of PHI (in any form) shall promptly be made to the Covered Entity in writing without unreasonable delay but in no event not later than thirty (30) business days from the date that Business Associate became aware of such alleged unauthorized uses or disclosures, or by exercising reasonable diligence should have known of such alleged

unauthorized uses or disclosures. Furthermore, in the event of an unauthorized use or disclosure of PHI, Business Associate shall mitigate, to the extent practicable, any harmful effects of said use or disclosure that are or should be known to it.

- (b) Instructions for Reporting a Breach. If reportable Breach under HIPAA occurs, Business Associate will notify Covered Entity, and in such notification, the Business Associate shall include, without limitation, to the extent possible the following information: (1) a brief description of what happened, including the date of the incident and the date of the discovery of the incident; (2) the identification of each individual whose PHI was compromised or potentially compromised; (3) a description of the types of PHI that were involved in the incident; (4) any steps individuals should take to protect themselves from potential harm resulting from the incident; and (5) a brief description of what Business Associate is doing to investigate the incident, to mitigate compromising the PHI, and to protect against any further incidents. If any such information is not available at the time of the notification, Business Associate shall work with Covered Entity to provide further information promptly thereafter as information becomes available.

#### 4. Compliance Related Changes.

The Parties recognize that HIPAA may change or may be clarified from time to time, and that terms of this Agreement may need to be revised, on advice of counsel, in order to remain in compliance with such changes or clarifications, and the Parties agree to negotiate, in good faith, revisions to the term or terms that cause the potential or actual violation or noncompliance. In the event either of the Parties, acting reasonably, is unable to agree to new or modified terms as required to bring the entire Agreement into compliance, either party may terminate this Agreement on thirty (30) days written notice to the other Party, or earlier if necessary to prevent noncompliance with a deadline or effective date or to protect any PHI at issue, as well as ensure compliance with all obligations under any of these procedures, rules, regulations or laws.

#### 5. Term and Termination.

- (a) Term. This Agreement shall become effective on the Effective Date set forth above and shall terminate upon the termination or expiration of the Agreement and when all PHI provided by either Party to the other, or created or received by Business Associate on behalf of Customer is, in accordance with this Section, destroyed or returned to Customer or, if the Parties determine that it is not feasible to return or destroy PHI, protections are extended to such information, in accordance with the terms of this Agreement.
- (b) Termination. Notwithstanding any other provision of any agreement, either Party may immediately terminate this Agreement if either Party, acting reasonably, makes the determination that the other Party has breached a material term of this BAA and has failed to remedy such breach within thirty (30) days after receipt of written notice thereof. At the termination of the Agreement, or of the uses and/or disclosures of the PHI by the Business Associate, Business Associate shall if feasible, return or allow the Covered Entity to destroy all PHI received from, created by, or maintained by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form in connection with this BAA through an automatic deletion option provided by the Business Associate and retain no copies of such information.

#### 6. Miscellaneous.

- (a) Integration and Sharing. Business Associate's service permits the integration, sharing, and exchange of information with Third Party Services and links (both, as defined in the Agreement) that may or may not be compliant with HIPAA. If the Covered Entity chooses to use such Third Party Service and/or Links, Covered Entity is solely liable and responsible for the exchange of information, including any PHI between the Business Associate's services and the third party. Third Party Service providers do not provide services on behalf of monday.com and are not Business Associates of monday.com. monday.com hereby expressly disclaims any liability for any use, disclosure, or other action taken by such Third Party Service providers or any noncompliance by Covered Entity with any applicable law, regulation, or contractual provision relating to the sharing of information, including PHI, with any such Third Party Service.
- (b) Audits. If and to the extent required to comply with applicable law, Business Associate shall provide to Covered Entity (and Covered Entity's regulators) access at reasonable hours and upon reasonable notice to, and coordination with, Business Associate's personnel, to the facilities at or from which services related to PHI are then being provided, and to Business Associate's records and other pertinent information, all to the extent relevant to audit Business Associate's compliance with its obligations under this Agreement. Business Associate shall provide any assistance reasonably requested by Covered Entity or its designee in conducting any such audit.
- (c) No Third-Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.

Business Associate agrees to comply with all of the requirements and to incorporate the requirements in its own agreements to the extent required by law. This Agreement supersedes any previous HIPAA Business Associate Agreement between the Parties related to the subject matter herein.

Last Update July 25, 2019