

## Wiz Business Associate Agreement

BY ACCEPTING THIS BAA, CUSTOMER IS ACCEPTING THE TERMS AND CONDITIONS FOR THIS BAA WITH RESPECT TO BOTH A FREE EVALUATION AND/OR A COMMERCIAL SUBSCRIPTION FOR THE SERVICES. BY ACCEPTING THIS BAA, YOU REPRESENT AND WARRANT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND YOUR ORGANIZATION TO THIS BAA. IF YOU DO NOT HAVE THIS AUTHORITY, DO NOT ACCEPT THIS BAA.

**THIS BUSINESS ASSOCIATE AGREEMENT/ ADDENDUM ("BAA")** amends the Wiz Subscription Agreement or other agreement for Wiz services entered into between the Parties (the "**Agreement**") between the Wiz entity that entered into the Agreement ("**Wiz**") and Customer pursuant to the Agreement. Each of Wiz and Customer may be referred to herein as a "**Party**" and together as the "**Parties**". This BAA forms a binding legal agreement to reflect the Parties' agreement with regard to processing Protected Health Information (as defined below).

### 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 applicable requirements thereof regarding the confidentiality and privacy of Protected Health Information.

(B) Wiz is a "Business Associate" or "Subcontractor" as such terms are defined under HIPAA, and provides to Customer certain services ("**Services**") pursuant to the Agreement. In connection with the Services, the parties anticipate that Wiz may from time to time create and/or 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, Wiz shall become a "Business Associate" or "Subcontractor" of Customer and will therefore have obligations regarding the confidentiality and privacy of Protected Health Information that Wiz creates for, or receives from or on behalf of, Customer.

(D) This BAA applies only to the extent that Customer is also a "Business Associate" or "Covered Entity," as that term is defined by HIPAA.

## 1. Definitions

1.1 For the purposes of this BAA, capitalized terms shall 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.

**"Health Insurance Portability and Accountability Act"** or "**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996 and regulations promulgated thereunder.

**"Health Information Technology for Economic and Clinical Health Act"** or "**HITECH Act**" means the security provisions of the American Recovery and Reinvestment Act of 2009, also known as the Health Information Technology for Economic and Clinical Health Act.

**“Protected Health Information”** or **“PHI”** is any information, whether oral or recorded in any form or medium that is created, received, maintained, or transmitted by Wiz for or on behalf of Customer, that identifies an individual or might reasonably be used to identify an individual and relates to: (i) the individual’s past, present or future physical or mental health; (ii) the provision of health care to the individual; or (iii) the past, present or future payment for health care.

**“Secretary”** shall refer to the Secretary of the U.S. Department of Health and Human Services.

**“Unsecured PHI”** shall 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.

## 2. Wiz Obligations

### 2.1 Use and Disclosure of PHI.

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

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

(c) Subject to the restrictions set forth in this BAA, Wiz may disclose PHI for the proper management and administration of Wiz, provided that:

(i) Such disclosures are required by law, or

(ii) Wiz obtains reasonable assurances from the person or entity to whom the information is disclosed that such information will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person or entity, and the person or entity notifies the Wiz of any instances of which it is aware in which the confidentiality of the information has been breached.

(d) Wiz 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 Wiz pursuant to this BAA with PHI, as defined by 45 C.F.R. 160.103, received by Wiz 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.

(e) Wiz may de-identify any and all PHI created or received by Wiz 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.

2.2 Safeguards. Wiz shall 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. Wiz shall 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.

2.3 Audits and Records. Wiz shall, in accordance with HIPAA, make available to the Secretary Wiz’s internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Wiz on behalf of, Customer for purposes of

determining Customer's compliance with its obligations under HIPAA.

#### 2.4 Individuals' Rights to Their PHI:

(a) To the extent Wiz 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, Wiz, within ten (10) business days upon receipt of written request by Customer, shall make available to Customer such PHI.

(i) In the event that any Individual requests access to PHI directly from Wiz, Wiz shall forward such request to Customer within five (5) business days.

(ii) Customer will be responsible for making all determinations regarding the grant or denial of an Individual's request for PHI and Wiz 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 Wiz by Customer, shall be the responsibility of Customer, including resolution or reporting of all appeals and/or complaints arising from denials.

(b) To the extent Wiz 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, Wiz shall, within ten (10) business days upon receipt of a written request by Customer, make available to Customer such PHI:

(i) In the event that any Individual requests amendment of PHI directly from Wiz, Wiz shall forward such request to Customer within five (5) business days.

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

(iii) Within ten (10) business days of receipt of a request from Customer to amend an individual's PHI in the Designated Record Set, Wiz shall 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.

(c) In order to allow Customer to respond to a request by an Individual for an accounting pursuant to 45 CFR Section 164.528, Wiz shall, 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.

(d) At a minimum, Wiz shall, to the extent known by Wiz, 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.

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

(ii) Customer will be responsible for preparing and delivering an accounting to Individual.

(iii) Wiz shall implement an appropriate record keeping process to enable it to comply with the requirements of this BAA.

(e) Disclosure to Third Parties. Wiz shall 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, Wiz for or on behalf of Customer, pursuant to which agreement such subcontractor and agent agrees to be bound by the same restrictions, terms, and conditions that apply to Wiz pursuant to this Agreement with respect to such PHI.

(f) Reporting Obligations.

(i) In the event of Wiz's discovery of any actual, alleged or reasonably suspected incident of unauthorized or accidental disclosure of or access to any Unsecured PHI that Wiz accesses, maintains, retains, modifies, records, or otherwise holds or uses on behalf of Customer ("**Security Breach**"), Wiz shall promptly report such Security Breach to Customer, without undue delay after the Security Breach is discovered and in accordance with applicable laws. Notice of a Security Breach shall 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 Security Breach, if known, and the date of discovery of the Security Breach; (3) the scope of the Security Breach; and (4) the Wiz's response to the Security Breach.

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

(iii) The parties acknowledge that unsuccessful Security Breaches (e.g., pings and other broadcast attacks on a firewall, denial of service attacks, port scans, unsuccessful login attempts) occur within the normal course of business and the parties stipulate and agree that this paragraph constitutes notice by Wiz to Customer for such unsuccessful Security Breaches.

### **3. Customer Obligations**

#### **3.1 Permissible Requests.**

(a) Customer shall not request Wiz 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.

(b) Customer shall be compliant with all applicable laws and regulations pertaining to PHI Customer sends, or directs to be sent, to Wiz.

#### **3.2 Notifications.**

(a) Customer shall notify Wiz 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 Wiz's use or disclosure of PHI.

(b) Customer shall notify Wiz of any changes in, or revocation of, permission by individual to use or disclose PHI, to the extent that such changes may affect Wiz's use or disclosure of PHI.

(c) Customer shall notify Wiz 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 Wiz's use or disclosure of PHI.

### **4. Term and Termination**

4.1 **Material Breach.** Where either party has knowledge of a material breach by the other party, the non-breaching party shall 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 thirty (30) days of the breaching party's receipt of notice from the non-breaching party of said breach, the non-breaching party may, 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 shall, if feasible, terminate this BAA and the portion(s) of the Agreement affected by the breach.

4.2 **Return or Destruction of PHI.** Upon termination of this BAA, Wiz shall:

(a) If feasible as determined by Wiz, return or destroy all PHI received from, or created or received by Wiz for or on behalf of Customer that Wiz or any of its subcontractors and agents still maintain, and Wiz shall retain no copies of such information; or

(b) If Wiz 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 Wiz's obligations under this Section 4.2 shall survive the termination of this BAA.

### **5. General**

5.1 Updates. Wiz may update this BAA and such updates will be made available at [www.wiz.io/legal/legal-hub](http://www.wiz.io/legal/legal-hub) (or any successor page(s)). Except for any updates required to comply with applicable law, which shall become effective immediately, any updates to the BAA shall become effective for Customer upon the earlier of (i) the renewal of Customer's then-current Subscription Term or (ii) upon the effective date of a new Order entered into by Customer. Wiz will notify Customer of any material updates to the BAA if Customer has subscribed to receive such updates via the "Legal Contact" within the Platform settings.

5.2 Interpretation. Any ambiguity in this BAA shall be resolved to permit the parties to comply with HIPAA and the HITECH Act. If any provision of this BAA is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

5.3 Limitation of Liability. The parties agree and acknowledge that the limitation of liability provisions contained under the Agreement shall apply and govern each party's performance under this BAA. NOTWITHSTANDING THE FOREGOING, IF CUSTOMER IS USING THE SERVICES FOR A FREE TRIAL, WIZ'S MAXIMUM AGGREGATE LIABILITY TO CUSTOMER UNDER THIS BAA SHALL BE CAPPED AT ONE THOUSAND DOLLARS US (\$1,000 US).

5.4 Conflicting Terms. In the event that any terms of this BAA conflict with any terms of the Agreement, the terms of this BAA shall govern and control over the conflicting term in the Agreement. All other nonconflicting terms of the Agreement shall remain valid and enforceable.

5.5 No waiver. The failure of either Party to enforce any rights granted hereunder or to take action against the other Party in the event of any breach hereunder shall not be deemed a waiver by that Party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

5.6 Governing Law and Jurisdiction. This BAA shall be governed by and construed under the laws of the state set forth in the Agreement.

5.7 Counterparts and Signatures. This Agreement may be executed in traditional or electronic counterparts, which together shall be deemed one instrument.