

HIPAA Business Associate Agreement

If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Data, GTB Hosting Data, or Professional Services Data, this HIPAA Business Associate Agreement (“BAA”) forms part of the GTB Software License and Services Agreement or other similar written or electronic agreement between GTB Technologies, Inc. on behalf of itself and its Affiliates (“GTB”) and Customer (the “**Agreement**”) to reflect the parties’ obligations with respect to the processing and security of Protected Health Information (as defined below) during the term of the Agreement. If there is any conflict between a provision in this BAA and a provision in the Agreement regarding PHI data, then this BAA will control, else the Agreement shall control as to all other terms and conditions.

1. Definitions.

Except as otherwise defined in this BAA, capitalized terms shall have the definitions set forth in HIPAA, and if not defined by HIPAA, such terms shall have the definitions set forth in the Agreement.

“Breach Notification Rule” **shall** mean the rule regarding notification obligations in the event of a Breach of Unsecured Protected Health Information (45 C.F.R. Parts 160 and 164, Subpart D).

“Business Associate” shall have the same meaning as the term “business associate” in 45 CFR § 160.103 of HIPAA.

“Covered Entity” shall have the same meaning as the term “covered entity” in 45 CFR § 160.103 of HIPAA.

“Customer”, for this BAA only, means Customer.

“GTB” means GTB Technologies, Inc. and its Affiliates.

“GTB Data” means all data, and software, that are provided to GTB by or on behalf of Customer for GTB’s performance of the GTB Services.

“GTB Services” means the onboarding, implementation and support services for software services that are provided to Customer by GTB in connection with Customer’s GTB SaaS subscription, excluding services that are performed using third-party software or software that is not hosted by GTB.

“HIPAA” collectively means the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations, including the Privacy Rule, the Breach Notification Rule, and the Security 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.

“GTB BAA-Scope Services”, for this BAA only, means the GTB Online Services as defined in the Product Terms incorporated into the Agreement.

“Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164, Subparts A and E),

“Professional Services” has the meaning provided in the GTB Agreement For clarity, the Professional Services in scope for this BAA are the GTB Software technical support as described in the Agreement.

“Professional Services Data” means all data, that are provided to GTB, by or on behalf of a customer (or that Customer authorizes GTB to obtain from an Online Service) or otherwise obtained or processed by or on behalf of GTB through an engagement with GTB to obtain Professional Services.

“Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103 of HIPAA, provided that it is limited to such protected health information that is received by GTB from, or created, received, maintained, or transmitted by GTB on behalf of, Customer (a) through the use of the GTB BAA-Scope Services, or (b) through GTB’s provision of Professional Services.

“Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A and C).

2. *Permitted Uses and Disclosures of Protected Health Information.*

- a. Performance of the Agreement.** Except as otherwise limited in this BAA, GTB may Use and Disclose Protected Health Information for, or on behalf of, Customer as specified in the Agreement; provided that any such Use or Disclosure would not violate HIPAA if done by Customer, unless expressly permitted under paragraph b of this Section.
- b. Management, Administration, and Legal Responsibilities.** Except as otherwise limited in this BAA, GTB may Use and Disclose Protected Health Information solely as necessary for the proper internal management and administration of GTB and/or to carry out its legal responsibilities, provided that such Use or Disclosure complies with the minimum necessary standard under HIPAA.

3. *Responsibilities of the Parties with Respect to Protected Health Information.*

- a. GTB’s Responsibilities.** To the extent GTB is acting as a Business Associate, GTB agrees to the following:
 - (i) Limitations on Use and Disclosure.** GTB shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Agreement and/or this BAA or as otherwise Required by Law. GTB shall not disclose, capture, maintain, scan, index, transmit, share or Use Protected Health Information for any activity not authorized under the Agreement and/or this BAA. GTB BAA-Scope Services, and Professional Services shall not use Protected Health Information for any advertising, marketing or similar commercial purpose of GTB or any third party. GTB shall not violate the HIPAA prohibition on the sale of Protected Health Information. GTB shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.
 - (ii) Safeguards.** GTB shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.
 - (iii) Reporting.** GTB shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which GTB becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer’s

Unsecured Protected Health Information that GTB may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made without unreasonable delay, and in no event later than five (5) business days after GTB's confirmation of a Breach.. Taking into account the level of risk reasonably likely to be presented by the Use, Disclosure, Security Incident, or Breach, the timing of other reporting will be made consistent with GTB's and Customer's legal obligations.

For purposes of this Section, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on GTB's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information. Notification(s) under this Section, if any, will be delivered to contacts identified by Customer pursuant to Section 3b(ii) (Contact Information for Notices) of this BAA by any means GTB selects, including through e-mail. GTB's obligation to report under this Section is not and will not be construed as an acknowledgement by GTB of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

- (iv) Subcontractors.** In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, GTB shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of GTB to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to GTB with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule. GTB remains responsible for its Subcontractors' compliance with obligations in this BAA.
- (v) Disclosure to the Secretary.** GTB shall make available its internal practices, records, and books directly related to the Use and/or Disclosure of Protected Health Information received from Customer, to the extent required by law and subject to applicable legal privileges, including attorney-client and trade secret protections.
- (vi) Access.** The parties acknowledge and agree that GTB does not maintain Protected Health Information in a Designated Record Set for Customer. In the event that there is a change in the GTB BAA-Scope Services, or Professional Services that GTB provides to Customer such that GTB commences maintaining Protected Health Information in a Designated Record Set, then GTB, at the request of Customer, shall within fifteen (15) days make access to such Protected Health Information available to Customer in accordance with 45 CFR § 164.524 of the Privacy Rule.
- (vii) Amendment.** Subject to Section 3a(vi) above, if GTB maintains Protected Health Information in a Designated Record Set for Customer, then GTB, at the request of Customer, shall within fifteen (15) days make available such Protected Health Information to Customer for amendment and incorporate any reasonably requested amendment in the Protected Health Information in accordance with 45 CFR § 164.526 of the Privacy Rule.
- (viii) Accounting of Disclosure.** GTB, at the request of Customer, shall within thirty (30) days make available to Customer such information relating to Disclosures made by GTB as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.

- (ix) **Performance of a Covered Entity's Obligations.** To the extent GTB is to carry out a Covered Entity obligation under the Privacy Rule, GTB shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.
- (x) Section 3(a)(vi–viii): Designated Record Set Clauses Notwithstanding the foregoing, GTB does not intend to create or maintain a Designated Record Set and shall not be responsible for such obligations unless explicitly agreed in writing by the parties.

b. Customer Responsibilities.

- (i) **No Impermissible Requests.** Customer shall not request GTB to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).
- (ii) **Contact Information for Notices.** Customer hereby agrees that any reports, notification, or other notice by GTB pursuant to this BAA will be provided as set forth in the Agreement or associated order form / or invoice.
- (iii) **Safeguards and Appropriate Use of Protected Health Information.** Customer is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Customer's obligation to:
 - 1) Not include Protected Health Information in: (1) information Customer submits to technical support personnel through a technical support request or to community support forums outside of Professional Services, or, for Professional Services, within the subject or body of a support case management or support ticket; and (2) Customer's address book or directory information. In addition, GTB does not act as, or have the obligations of, a Business Associate under HIPAA with respect to Customer Data, or Professional Services Data once it is sent to or from Customer outside GTB BAA-Scope Services, or Professional Services over the public Internet, or if Customer fails to follow applicable instructions regarding physical media transported by a common carrier.
 - 2) During use of GTB BAA-Scope Services or in an engagement with GTB to obtain Professional Services or implement privacy and security safeguards in the systems, applications, and software that Customer controls, configures, and uploads.

4. Applicability of BAA.

This BAA is applicable to GTB BAA-Scope Services, and Professional Services as it relates to PHI data. GTB may, from time to time, (a) include additional GTB online services in the GTB Products and Services and (b) update the definition of GTB BAA-Scope Services, and Professional Services in this BAA, and such updated definitions will apply to Customer without additional action by Customer. It is Customer's obligation to not store or process in an online service, or provide to GTB for performance of a professional service, protected health information (as that term is defined in 45 CFR § 160.103 of HIPAA) until this BAA is effective as to the applicable service.

5. Term and Termination.

- a. **Term.** This BAA shall continue in effect until the earlier of (1) termination by a Party for breach as set forth in Section 5.b., below, or (2) expiration of Customer's Agreement.
- b. **Termination for Breach.** Upon written notice, either Party immediately may terminate the Agreement and this BAA if the other Party is in material breach or default of any obligation in this BAA. Either party may provide the other a thirty (30) calendar day period to cure a material breach or default within such written notice.
- c. **Return, Destruction, or Retention of Protected Health Information Upon Termination.** Upon expiration or termination of this BAA, GTB shall return or destroy all Protected Health Information in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Agreement. If it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this BAA then GTB shall extend the protections of this BAA to such Protected Health Information for a period not to exceed twelve (12) months, unless a longer retention period is required by applicable law.

6. ***Miscellaneous.***

- a. **Interpretation.** The Parties intend that this BAA be interpreted consistently with their intent to comply with HIPAA and other applicable federal and state law. Except where this BAA conflicts with the Agreement, all other terms and conditions of the Agreement remain unchanged. Any captions or headings in this BAA are for the convenience of the Parties and shall not affect the interpretation of this BAA.
- b. **Amendments; Waiver.** This BAA may not be modified or amended except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, as a bar to, or as a waiver of any right or remedy as to subsequent events.
- c. **No Third-Party Beneficiaries.** Nothing express or implied in this BAA is intended to confer, nor shall anything in this BAA confer, upon any person other than the Parties, and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.
- d. **Severability.** In the event that any provision of this BAA is found to be invalid or unenforceable, the remainder of this BAA shall not be affected thereby, but rather the remainder of this BAA shall be enforced to the greatest extent permitted by law.
- e. **No Agency Relationship.** It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Customer and GTB under HIPAA or the Privacy Rule, Security Rule, or Breach Notification Rule. No terms or conditions contained in this BAA shall be construed to make or render GTB an agent of Customer. The parties agree that GTB is acting as an independent contractor and shall not be deemed an agent of the Customer under HIPAA or any other applicable law.
- f. **Right to Modify.** This BAA may be updated to reflect legal or operational requirements. GTB will provide notice of material changes via <https://gttb.com/wp-content/uploads/2025/06/HIPAA%20Business%20Associate%20Agreement%20-%20GTB.pdf> and Customer's continued use of the services constitutes acceptance.