

BUSINESS ASSOCIATE AGREEMENT

Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and their implementing regulations at 45 CFR Parts 160 and 164

This Business Associate Agreement ("**Agreement**" or "**BAA**") is entered into as of the date of last signature below (the "**Effective Date**") by and between:

COVERED ENTITY:

(Practice / Organization Name)

(Address)

**BUSINESS
ASSOCIATE:**

Meridian Billing Services LLC
101 Arch Street, 8th Floor
Boston, MA 02110
EIN: 92-0406352

The Covered Entity and Business Associate are each a "**Party**" and collectively the "**Parties**." This Agreement supplements and is made a part of the Service Agreement between the Parties for medical billing, revenue cycle management, insurance credentialing, and/or MICRA-BEV platform services (the "**Service Agreement**").

RECITALS

WHEREAS, the Parties have entered into, or intend to enter into, a Service Agreement under which Business Associate may create, receive, maintain, or transmit Protected Health Information ("PHI") on behalf of Covered Entity; and

WHEREAS, the Parties intend to comply with the requirements of HIPAA, the HITECH Act, and the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule as set forth in 45 CFR Parts 160 and 164; and

WHEREAS, the purpose of this Agreement is to set forth the terms and conditions pursuant to which PHI will be handled by Business Associate in the course of performing services under the Service Agreement;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. DEFINITIONS

"**Breach**" shall have the meaning given to such term under 45 CFR §164.402.

"**Business Associate**" shall have the meaning given to such term under 45 CFR §160.103.

"**Covered Entity**" shall have the meaning given to such term under 45 CFR §160.103.

"**Designated Record Set**" shall have the meaning given to such term under 45 CFR §164.501.

"**Electronic Protected Health Information**" ("**ePHI**") shall have the meaning given to such term under 45 CFR §160.103.

"**Individual**" shall have the meaning given to such term under 45 CFR §160.103 and shall include a person who qualifies as a personal representative per 45 CFR §164.502(g).

"**Protected Health Information**" ("**PHI**") shall have the meaning given to such term under 45 CFR §160.103, limited to the information created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

"**Required by Law**" shall have the meaning given to such term under 45 CFR §164.103.

"**Secretary**" means the Secretary of the United States Department of Health and Human Services or designee.

"**Security Incident**" shall have the meaning given to such term under 45 CFR §164.304.

"**Subcontractor**" shall have the meaning given to such term under 45 CFR §160.103.

"**Unsecured PHI**" shall have the meaning given to such term under 45 CFR §164.402.

All other terms used but not otherwise defined in this Agreement shall have the meanings set forth in 45 CFR Parts 160 and 164, as amended from time to time.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

(a) Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement, the Service Agreement, or as Required by Law.

(b) Business Associate agrees to use appropriate administrative, physical, and technical safeguards, and comply with Subpart C of 45 CFR Part 164, to prevent use or disclosure of PHI other than as provided for by this Agreement.

(c) Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, including any Security Incident or Breach of Unsecured PHI, as further described in Section 4 below.

(d) Business Associate agrees, in accordance with 45 CFR §164.502(e)(1)(ii) and §164.308(b)(2), to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate under this Agreement. Business Associate's current Subcontractors include clearinghouse partners (Availity, CLAIM.MD) and communications infrastructure providers (Twilio), each of which maintains a BAA with Business Associate.

(e) Business Associate agrees to make available PHI in a Designated Record Set to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 CFR §164.524, within fifteen (15) business days of a written request.

(f) Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by Covered Entity pursuant to 45 CFR §164.526, within fifteen (15) business days of a written request.

(g) Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy the Covered Entity's obligations under

45 CFR §164.528, within thirty (30) days of a written request.

- (h) Business Associate agrees to make its internal practices, books, and records available to the Secretary of HHS for purposes of determining compliance with HIPAA.
- (i) Business Associate agrees to implement the minimum necessary standard, using or disclosing only the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure.
- (j) Business Associate agrees to encrypt all ePHI in transit using TLS 1.3 (or successor standard) and at rest using AES-256 encryption, in accordance with NIST Special Publication 800-111 and the HHS Guidance Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.
- (k) Business Associate agrees to maintain comprehensive audit logs of all access to and modifications of PHI, retaining such logs for a minimum of six (6) years.
- (l) Business Associate agrees not to store PHI in application logs, debugging output, analytics systems, or any system not specifically designated and secured for PHI storage.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Service Agreement, provided that such use or disclosure would not violate HIPAA if done by Covered Entity. Specifically:

- (a) Business Associate may use PHI to provide medical billing, revenue cycle management, insurance credentialing, multi-state licensure, payer contracting, and MICRA-BEV insurance verification services as described in the Service Agreement.
- (b) Business Associate may use or disclose PHI as Required by Law.
- (c) Business Associate may use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities, provided that any disclosures are Required by Law, or Business Associate obtains reasonable assurances from the recipient that the PHI will remain confidential and will be used or disclosed only as Required by Law or for the purposes for which it was disclosed.
- (d) Business Associate may de-identify PHI in accordance with 45 CFR §164.514(a)-(c). De-identified data is not subject to the terms of this Agreement.
- (e) Business Associate may transmit PHI to clearinghouse partners (currently Availity and CLAIM.MD) for the sole purpose of processing EDI 270/271 eligibility transactions, limited to the minimum necessary information required for such transactions.

4. BREACH NOTIFICATION

- (a) Business Associate shall report to Covered Entity any Breach of Unsecured PHI without unreasonable delay, and in no case later than **thirty (30) calendar days** after discovery of the Breach. Discovery occurs on the first day the Breach is known to Business Associate or, by exercising reasonable diligence, would have been known.

- (b) Business Associate's notification shall include, to the extent available: (i) identification of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed during the Breach; (ii) a description of the nature of the Breach, including the types of Unsecured PHI involved; (iii) the date of the Breach and date of discovery; (iv) a description of what Business Associate is doing to investigate, mitigate harm, and protect against further Breaches; and (v) contact information for individuals who can answer questions about the Breach.
- (c) Business Associate shall cooperate with Covered Entity in investigating the Breach and in meeting Covered Entity's obligations under the Breach Notification Rule (45 CFR §§164.404-164.408).
- (d) Business Associate shall report any Security Incident of which it becomes aware. The Parties acknowledge that unsuccessful attempts at unauthorized access (such as port scans, unsuccessful login attempts, or pings) occur routinely and do not constitute Security Incidents requiring individual notification. Business Associate shall provide a summary report of such unsuccessful attempts upon Covered Entity's written request.

5. OBLIGATIONS OF COVERED ENTITY

- (a) Covered Entity shall notify Business Associate of any limitation(s) in the Covered Entity's notice of privacy practices under 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- (b) Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- (c) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
- (d) Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

6. TERM AND TERMINATION

- (a) **Term.** This Agreement shall be effective as of the Effective Date and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity. If it is infeasible to return or destroy all PHI, the protections of this Agreement shall extend to such PHI.
- (b) **Termination for Cause.** Either Party may terminate this Agreement if it determines that the other Party has materially breached this Agreement, provided that the breaching Party is given written notice and a thirty (30) day opportunity to cure the breach. If the breach is not cured within thirty (30) days, the non-breaching Party may terminate this Agreement. If cure is not possible, the non-breaching Party may terminate this Agreement immediately upon written notice.
- (c) **Effect of Termination.** Upon termination of this Agreement, Business Associate shall, if feasible, return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, that Business Associate still maintains in any form. Business Associate shall retain no copies of the PHI. If

return or destruction is infeasible, Business Associate shall notify Covered Entity and extend the protections of this Agreement to such PHI, limiting further uses and disclosures to those purposes that make the return or destruction infeasible.

(d) Survival. The obligations of Business Associate under Sections 2, 4, and 6(c) shall survive the termination of this Agreement.

7. MISCELLANEOUS

(a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended from time to time. The Parties agree to take such action as is necessary to amend this Agreement from time to time to comply with changes in HIPAA and its implementing regulations.

(b) Amendment. This Agreement may not be modified except by a written instrument signed by both Parties.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with HIPAA.

(d) Entire Agreement. This Agreement, together with the Service Agreement, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral, relating to the same.

(e) Governing Law. This Agreement shall be governed by and construed in accordance with federal law, including HIPAA and the HITECH Act. To the extent not preempted by federal law, the laws of the Commonwealth of Massachusetts shall apply.

(f) Severability. If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(g) No Third-Party Beneficiaries. Nothing in this Agreement shall confer upon any person other than the Parties and their respective successors or assigns any rights, remedies, obligations, or liabilities.

(h) Indemnification. Business Associate shall indemnify, defend, and hold harmless Covered Entity from and against any claims, losses, liabilities, costs, and expenses (including reasonable attorney's fees) arising out of or in connection with any Breach of Unsecured PHI caused by Business Associate's violation of this Agreement or applicable law.

IN WITNESS WHEREOF, the Parties have executed this Business Associate Agreement as of the Effective Date written below.

COVERED ENTITY

BUSINESS ASSOCIATE

Meridian Billing Services LLC

Signature

Signature

Printed Name

Printed Name

Title

Title

Date

Date

This document is provided as a standard Business Associate Agreement template by Meridian Billing Services LLC. Covered Entity should consult with legal counsel before execution.