

## BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (this “*Agreement*”) made as of this \_\_\_th day of \_\_\_\_\_, 20\_\_ by and between [ BUSINESS ASSOCIATE ], a [entity type and state where registered entity is registered] (“*Business Associate*”), and \_\_\_\_\_, a entity type and state where registered entity is registered] with a principal address of \_\_\_\_\_ (the “*Covered Entity*”).

### WITNESSETH:

WHEREAS, Business Associate provides various services related to \_\_\_\_\_, including without limitation an internet-based service known as “Business Associate” (the “*Business Associate Service*”); and

WHEREAS, the Covered Entity is a covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (the “*Act*”), Public Law 104-191, as modified by the Titles of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, known as the “Health Information Technology for Economic and Clinical Health Act” (“*HITECH Act*”) and the regulations promulgated thereunder and codified at 45 CFR Parts 160 and 164 (such regulations together with the Act and the HITECH Act, “*HIPAA*”); and

WHEREAS, as a “covered entity,” the Covered Entity must obtain reasonable and adequate assurances that any of its contractors who obtain, create, transmit, or maintain Protected Health Information (“*PHI*”), as defined below, on its behalf will abide by certain restrictions prescribed by HIPAA in the course of providing services; and

WHEREAS, in the course of performing the Business Associate Service pursuant to that certain Business Associate Master Services and License Agreement between the Covered Entity and Business Associate (the “*Master Agreement*”), Business Associate may have access to and require use of PHI; and

WHEREAS, the parties desire to establish the permissible and required uses and disclosures of PHI by Business Associate.

NOW, THEREFORE, the parties hereby agree as follows:

This agreement is being provided as an example of a business associate agreement (BAA). It is not recommended for use by a specific practice. Confer with your legal advisers to determine what is needed by your practice and to confirm that any agreement is legally sufficient and in line with both federal and/or state law where you practice. The authors and operators of this website make no warranties or guarantees regarding the legal sufficiency of this document for specific purposes. The titles, abbreviations, and other terminology in this sample BAA may need to be revised to fit your organization’s communication protocols or specific needs.

1. **Definitions.** All capitalized terms used but not defined herein shall have the meanings set forth in the HIPAA Rules, defined below. The following terms shall have the following specific meanings:

a. “*HIPAA Rules*” shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164.

b. “*PHI*” has the same meaning as the term “protected health information” at 45 CFR 160.103, limited to the PHI exchanged by the parties pursuant to this Agreement.

c. “*Covered Entity*” shall generally have the same meaning as the term “covered entity” defined at 45 CFR 160.103, and in reference to this Agreement, shall mean the Covered Entity named above.

2. **Obligations of Business Associate.** Business Associate shall:

a. Not use or disclose PHI except to the extent permitted or required by this Agreement or Required by Law.

b. Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of PHI other than as provided by this Agreement.

c. Report to Covered Entity, within thirty (30) business days after discovery, any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, including Breaches of Unsecured PHI as required by 45 CFR 164.410, and any Security Incident of which it becomes aware. Notwithstanding the foregoing, the parties acknowledge the ongoing existence and occurrence of inconsequential incidents that occur on a daily basis, such as scans, “pings,” or other unsuccessful attempts to penetrate computer networks or servers containing electronic PHI, and the parties agree that no notification by Business Associate of such unsuccessful Security Incidents is required.

d. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors of Business Associate that create, receive, maintain, or transmit PHI on behalf of Business Associate or the Covered Entity agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such PHI.

e. Make available to the Covered Entity PHI in a Designated Record Set within fifteen (15) days of the Covered Entity’s request, as necessary for the Covered Entity to satisfy its

This agreement is being provided as an example of a business associate agreement (BAA). It is not recommended for use by a specific practice. Confer with your legal advisers to determine what is needed by your practice and to confirm that any agreement is legally sufficient and in line with both federal and/or state law where you practice. The authors and operators of this website make no warranties or guarantees regarding the legal sufficiency of this document for specific purposes. The titles, abbreviations, and other terminology in this sample BAA may need to be revised to fit your organization’s communication protocols or specific needs.

obligations under 45 CFR 164.524. Business Associate shall refer all requests for access that it receives directly from an Individual to the Covered Entity.

f. Make any amendments to PHI in a Designated Record Set as directed by the Covered Entity, and within thirty (30) days of the Covered Entity's request, pursuant to 45 CFR 164.526, or take other measures as necessary for the Covered Entity to satisfy its obligations under 45 CFR 164.526. Business Associate shall refer all requests for amendment that it receives directly from an Individual to the Covered Entity.

g. Maintain and make available the information required to provide an accounting of disclosures to the Covered Entity within thirty (30) days of Covered Entity's request, as necessary for the Covered Entity to satisfy its obligations under 45 CFR 164.528. Business Associate shall refer all requests for an accounting of disclosures that it receives directly from an Individual to the Covered Entity.

h. At the Covered Entity's request and under the Covered Entity's direction, cooperate with the Covered Entity to fulfill the breach notification requirements under Subpart D of 45 CFR Part 164 for any breaches caused by Business Associate or involving PHI maintained by Business Associate.

i. Make its internal practices, books, and records available to the Secretary of Health and Human Services for purposes of determining compliance with the HIPAA Rules. Business Associate will promptly notify the Covered Entity of any governmental audits or investigations relating to the HIPAA Rules that are threatened or commenced against Business Associate, to the extent permissible under the HIPAA Rules and other applicable law.

j. Adequately train and inform its employees, contractors, agents, and representatives providing the Business Associate Service of the terms of this Agreement and their legal obligations to comply with this Agreement and the HIPAA Rules.

3. **Obligations of the Covered Entity**. The Covered Entity shall:

a. Upon request, provide Business Associate with its current notice of privacy practices adopted in accordance with the Privacy Regulations.

b. Inform Business Associate of any revocations, amendments, or restrictions in the use or disclosure of PHI if such changes affect Business Associate's permitted or required uses and disclosure of PHI hereunder.

This agreement is being provided as an example of a business associate agreement (BAA). It is not recommended for use by a specific practice. Confer with your legal advisers to determine what is needed by your practice and to confirm that any agreement is legally sufficient and in line with both federal and/or state law where you practice. The authors and operators of this website make no warranties or guarantees regarding the legal sufficiency of this document for specific purposes. The titles, abbreviations, and other terminology in this sample BAA may need to be revised to fit your organization's communication protocols or specific needs.

c. Use best efforts to only disclose to Business Associate the minimum amount of PHI necessary for Business Associate to provide its services to the Covered Entity.

d. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Covered Entity's PHI and minimize Business Associate's exposure to such information.

4. **Permitted Uses and Disclosures by Business Associate.** Business Associate may:

a. Use or disclose PHI to the extent necessary to provide the Business Associate Service. Any such use or disclosure will be consistent with the scope and limitations of the Master Agreement and the Covered Entity's privacy policies that are made known to Business Associate.

b. Use or disclose PHI to the extent Required by Law.

c. Not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by the Covered Entity, except as otherwise set forth in this Section 4.

d. Use and disclose PHI for its own proper management and administration or to carry out its legal responsibilities, provided the disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

e. Use, disclose, and request only the minimum amount of PHI necessary, and shall comply with any of the Covered Entity's minimum necessary policies that are provided to Business Associate. Business Associate shall comply with any future guidance published by the Department of Health and Human Services.

f. Provide data aggregation services relating to the Health Care Operations of the Covered Entity. Unless otherwise prohibited in the Master Agreement, Business Associate may de-identify PHI from the Covered Entity in accordance with 45 C.F.R. 164.514(a)-(c).

5. **Term and Termination.**

a. The term of this Agreement shall be effective as of the date first above written and shall terminate upon the termination of the Master Agreement or upon earlier termination pursuant to Section 4(b)-(c) below.

This agreement is being provided as an example of a business associate agreement (BAA). It is not recommended for use by a specific practice. Confer with your legal advisers to determine what is needed by your practice and to confirm that any agreement is legally sufficient and in line with both federal and/or state law where you practice. The authors and operators of this website make no warranties or guarantees regarding the legal sufficiency of this document for specific purposes. The titles, abbreviations, and other terminology in this sample BAA may need to be revised to fit your organization's communication protocols or specific needs.

b. In the event of any amendment or modification to the HIPAA Rules or any other statutory requirement, the parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after thirty (30) days of negotiations, the terms of this Agreement fail to comply with the HIPAA Rules or other statutory requirements, then this Agreement shall immediately terminate.

c. Either party may terminate this Agreement if it determines that the other party has violated a material term of the Agreement and the other party fails to cure the breach or end the violation within thirty (30) days of being notified of such breach or violation.

d. Upon the Covered Entity's request or upon termination of this Agreement, Business Associate shall, if feasible, return to the Covered Entity (or, if directed by the Covered Entity, destroy in compliance with the HIPAA Rules) all PHI received from the Covered Entity or created, maintained or received by Business Associate on behalf of the Covered Entity. If Business Associate believes that such return or destruction is not feasible, Business Associate shall notify the Covered Entity. Business Associate may thereafter retain such PHI, provided that Business Associate continues to comply with the provisions of this Agreement for so long as it maintains such PHI and further limits uses and disclosures of such PHI to those purposes that make return or destruction infeasible. Business Associate shall ensure that its subcontractors return, destroy, or protect all PHI in the same manner. Notwithstanding the foregoing, Business Associate shall not be obligated to return or destroy the PHI of any individual who has requested that Business Associate retain such PHI pursuant to the individual's right of access found in 45 C.F.R. § 164.524(a) following termination of this Agreement. The rights and obligations of Business Associate under this subsection 5(d) shall survive expiration or termination of this Agreement.

6. **Miscellaneous**. This Section shall survive the expiration or termination of this Agreement.

a. At all times, Business Associate will be acting as an independent contractor engaged by the Covered Entity to perform the Business Associate Service. Nothing contained in this Agreement shall be construed to create an employment relationship, partnership or joint venture or to authorize the parties to act as general or special agents of one another, except as specifically set forth in this Agreement or any other agreement between the parties.

b. This Agreement may not be modified or amended, except in writing as agreed to by each party.

c. In the event that a provision of this Agreement is contrary to a provision of any other agreement between the parties, the provisions of this Agreement shall control.

This agreement is being provided as an example of a business associate agreement (BAA). It is not recommended for use by a specific practice. Confer with your legal advisers to determine what is needed by your practice and to confirm that any agreement is legally sufficient and in line with both federal and/or state law where you practice. The authors and operators of this website make no warranties or guarantees regarding the legal sufficiency of this document for specific purposes. The titles, abbreviations, and other terminology in this sample BAA may need to be revised to fit your organization's communication protocols or specific needs.

d. Neither party may assign its respective rights and obligations under this Agreement without the prior written consent of the other party.

e. Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA.

f. In the event any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions will remain in full force and effect.

g. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

h. This Agreement will be governed by (insert State) law, without regard for its choice of law provisions.

i. Except as expressly stated herein or the HIPAA Rules, the parties do not intend to create any rights in any third parties.

j. This Agreement may be executed in counterparts and electronically.

IN WITNESS WHEREOF, the parties have caused this Business Associate Agreement to be executed by their duly authorized representatives as of the dates shown below.

[BUSINESS ASSOCIATE]

[COVERED ENTITY]

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date of Signature: \_\_\_\_\_

Date of Signature: \_\_\_\_\_

This agreement is being provided as an example of a business associate agreement (BAA). It is not recommended for use by a specific practice. Confer with your legal advisers to determine what is needed by your practice and to confirm that any agreement is legally sufficient and in line with both federal and/or state law where you practice. The authors and operators of this website make no warranties or guarantees regarding the legal sufficiency of this document for specific purposes. The titles, abbreviations, and other terminology in this sample BAA may need to be revised to fit your organization's communication protocols or specific needs.