***Instructions:***

* ***This is a SAMPLE Business Associate Agreement, the majority of which was provided by the Department of Health and Human Services that meets the latest HIPAA requirements.***
* ***Discuss this with your legal counsel to ensure you make the changes necessary to best fit the requirements of your own organization.***
* ***Delete any “Optional” passages that do not apply to the agreement between you and your Business Associate (BA) or Covered Entity (CE).***
* ***Modify the “Optional” passages you keep to reflect the specifics of your agreement with your BA or CE.***
* ***Delete the highlighted passages before executing the agreement, along with deleting this entire “Instructions” section.***

**1.22. SAMPLE Business Associate Agreement**

**Introduction <<NOTE: Delete this entire Introduction section, on pages 1 – 2, before using as an actual binding contract.>>**

A “Business Associate” is a person or entity, other than a member of the workforce of a Covered Entity, who performs functions or activities on behalf of, or provides certain services to, a Covered Entity that involve access by the Business Associate to PHI.  A “Business Associate” also is a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another Business Associate.  The HIPAA Rules generally require that Covered Entities and Business Associates enter into contracts with their Business Associates to ensure that the Business Associates will appropriately safeguard PHI.  The Business Associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of PHI by the Business Associate, based on the relationship between the parties and the activities or services being performed by the Business Associate.  A Business Associate may use or disclose PHI only as permitted or required by its Business Associate contract or as required by law.  A Business Associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of PHI that are not authorized by its contract or required by law. A Business Associate also is directly liable and subject to civil penalties for failing to safeguard electronic PHI in accordance with the HIPAA Security Rule.

A written contract between a Covered Entity and a Business Associate must:

(1) establish the permitted and required uses and disclosures of protected health information (PHI) by the Business Associate;

(2) provide that the Business Associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;

(3) require the Business Associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the PHI, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI;

(4) require the Business Associate to report to the Covered Entity any use or disclosure of the PHI not provided for by its contract, including incidents that constitute breaches of unsecured PHI;

(5) require the Business Associate to disclose PHI as specified in its contract to satisfy a Covered Entity’s obligation with respect to individuals' requests for copies of their associated PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings;

(6) to the extent the Business Associate is to carry out a Covered Entity’s obligation under the Privacy Rule, require the Business Associate to comply with the requirements applicable to the obligation;

(7) require the Business Associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity for purposes of HHS determining the Covered Entity’s compliance with the HIPAA Privacy Rule;

(8) at termination of the contract, if feasible, require the Business Associate to return or destroy all PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity;

(9) require the Business Associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the Business Associate with respect to such information; and

(10) authorize termination of the contract by the Covered Entity if the Business Associate violates a material term of the contract.  Contracts between Business Associates and Business Associates that are subcontractors are subject to these same requirements.

This document includes sample Business Associate agreement provisions to help Covered Entities and Business Associates more easily comply with the Business Associate contract requirements.  While these sample provisions are written for the purposes of the contract between a Covered Entity and its Business Associate, the language may be adapted for purposes of the contract between a Business Associate and subcontractor.

This is only sample language and use of these exact sample provisions is not required for compliance with the HIPAA Rules.  The language may, and should as necessary, be changed to more accurately reflect business arrangements between a Covered Entity and Business Associate or Business Associate and subcontractor.  In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a Covered Entity and Business Associate or Business Associate and subcontractor, or they may be incorporated into a separate Business Associate agreement. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract.  Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

**Business Associate Agreement Provisions**

   Words or phrases contained in brackets [] are intended as either optional language or as instructions to the users of these sample provisions.

**Definitions**

Catch-all definition:

    The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules (<https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the>): Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate.  “Business Associate” shall generally have the same meaning as the term “Business Associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity.  “Covered Entity” shall generally have the same meaning as the term “Covered Entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules.  “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

**Obligations and Activities of Business Associate**

Business Associate agrees to:

(a) Not use or disclose PHI other than as permitted or required by the Agreement or as 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 for by the Agreement;

(c) Report to Covered Entity any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of unsecured PHI as required at 45 CFR 164.410, within [Put the amount of time within which notice must be provided. Suggested timeframe is 48 hours, except for any specified breaches putting patients at immediate risk of harm, which should be reported as soon as possible] and any security incident of which it becomes aware;

[NOTE: The parties may wish to add additional specificity regarding the breach notification obligations of the Business Associate, such as a stricter timeframe for the Business Associate to report a potential breach to the Covered Entity and/or whether the Business Associate will handle breach notifications to individuals (which would typically not be recommended), the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the Covered Entity. Delete this passage within the brackets before executing this contract.]

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

(e) Make available PHI in a designated record set to the [Choose either “Covered Entity” or “individual or the individual’s designee”] as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.524;

[NOTE: The parties may wish to add additional specificity regarding how the Business Associate will respond to a request for access that the Business Associate receives directly from the individual (such as whether and in what time and manner a Business Associate is to provide the requested access or whether the Business Associate will forward the individual’s request to the Covered Entity to fulfill) and the timeframe for the Business Associate to provide the information to the Covered Entity. Delete this passage within the brackets before executing this contract.]

(f) Make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.526;

[NOTE: The parties may wish to add additional specificity regarding how the Business Associate will respond to a request for amendment that the Business Associate receives directly from the individual (such as whether and in what time and manner a Business Associate is to act on the request for amendment or whether the Business Associate will forward the individual’s request to the Covered Entity) and the timeframe for the Business Associate to incorporate any amendments to the information in the designated record set. Delete this passage within the brackets before executing this contract.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either “Covered Entity” or “individual”] as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.528;

[NOTE: The parties may wish to add additional specificity regarding how the Business Associate will respond to a request for an accounting of disclosures that the Business Associate receives directly from the individual (such as whether and in what time and manner the Business Associate is to provide the accounting of disclosures to the individual or whether the Business Associate will forward the request to the Covered Entity) and the timeframe for the Business Associate to provide information to the Covered Entity. Delete this passage within the brackets before executing this contract.]

(h)  To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

**Permitted Uses and Disclosures by Business Associate**

(a) Business Associate may only use or disclose PHI

[NOTE: Do one of the options below. Then, delete this passage within the brackets before executing this contract.]

[Option 1 – Provide a specific list of permissible purposes. Check with your organization’s lawyer if necessary to determine what such purposes would be.]

[Option 2 – Reference an underlying service agreement, such as “as necessary to perform the services set forth in Service Agreement.” Check with your lawyer about this.]

[NOTE: In addition to other permissible purposes, the parties should specify whether the Business Associate is authorized to use PHI to de-identify the information in accordance with 45 CFR 164.514(a)-(c).  The parties also may wish to specify the manner in which the Business Associate will de-identify the information and the permitted uses and disclosures by the Business Associate of the de-identified information. Delete this passage within the brackets before executing this contract.]

(b) Business Associate may use or disclose PHI as required by law.

(c) Business Associate agrees to make uses and disclosures and requests for PHI.

[Option 1] consistent with Covered Entity’s minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the Covered Entity’s minimum necessary policies and procedures.]

(d) Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity [NOTE: if the Agreement permits the Business Associate to use or disclose PHI for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add “, except for the specific uses and disclosures set forth below.”]

(e) [Optional] Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(f) [Optional] Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, 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 information has been breached.

(g) [Optional] Business Associate may provide data aggregation services relating to the health care operations of the Covered Entity.

**Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions**

(a) [Optional] Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of PHI.

(b) [Optional] 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 p PHI, to the extent that such changes may affect Business Associate’s use or disclosure of PHI.

(c) [Optional] 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.

**Permissible Requests by Covered Entity**

    [Optional] Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity. [Include an exception if the Business Associate will use or disclose PHI for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the Business Associate.]

**Term and Termination**

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement [and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity].  [Bracketed language may be added if the Covered Entity wishes to provide the Business Associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – use this if the Business Associate is to return or destroy all PHI upon termination of the agreement]

Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity [or, if agreed to by Covered Entity, destroy] all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form.  Business Associate shall retain no copies of the PHI.

[Option 2—use this if the agreement authorizes the Business Associate to use or disclose PHI for its own management and administration or to carry out its legal responsibilities and the Business Associate needs to retain PHI for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the remaining PHI that the Business Associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
4. Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under “Permitted Uses and Disclosures By Business Associate”] which applied prior to termination; and
5. Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the Business Associate will transmit the PHI to another Business Associate of the Covered Entity at termination, and/or could add terms regarding a Business Associate’s obligations to obtain or ensure the destruction of PHI created, received, or maintained by subcontractors.]

(d) Survival.  The obligations of Business Associate under this Section shall survive the termination of this Agreement.

**Right to Audit [Optional, but Highly Recommended. Modify this section as appropriate for the contracted activity and organization.]**

1. Covered Entity reserves the right to audit the Business Associate and information security controls and processes of any associated Service Providers and to perform relevant tests to ensure that it is compliant with applicable HIPAA information security and privacy requirements as well as the requirements within this contract. Business Associate will permit the Covered Entity to perform an information security audit, including an audit of technical, physical and administrative security of any applicable Service Provider premises applicable to the engagement and will cooperate and furnish all requested materials in a timely manner, within no more than [recommend putting “three” here, but use whatever is most appropriate for the business relationship] business days.
2. When requested, Business Associate agrees to provide evidence of compliance, such as through an independent information security review or audit commensurate with the requirements of this contract. This audit must be completed within a time frame specified by the Covered Entity.
3. [Optional] Covered Entity will obtain a completed compliance attestation from Business Associate each [put “month” or “quarter” depending upon the level of risk with the BA]. Covered Entity will arrange provision of the attestation to the Business Associate.
4. [Optional] Covered Entity will obtain [describe any other types of compliance validation requirements here] from the Business Associate each [put “month” or “quarter” depending upon the level of risk with the BA].

**Miscellaneous**

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

1. No Third Party Beneficiaries. There are no intended third party beneficiaries to this Agreement.
2. Without in anyway limiting the foregoing, it is the parties’ specific intent that nothing contained in this Agreement give rise to any right or cause of action, contractual or otherwise, in or on behalf of any Individual whose PHI is Used or Disclosed pursuant to this Agreement.
3. References. A reference in this Agreement to a section in HIPAA means the section as in effect or as amended, and for which compliance is required.
4. Amendment. No amendment to this Agreement shall be effective until reduced to writing and signed by the parties. Notwithstanding the foregoing, this Agreement shall be deemed automatically amended to the extent necessary for Covered Entity to continue to comply with the requirements of HIPAA and its implementing regulations, as those requirements may be amended from time to time.
5. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Entity, in the opinion of its counsel, to comply with HIPAA.
6. Waiver. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.
7. Authority. The persons signing below have the right and authority to execute this Agreement for their respective entities and no further approvals are necessary to create a binding Agreement.
8. Conflict. In the event of any conflict between the terms and conditions stated within this Agreement and those contained within any other agreement or understanding between the parties, written, oral or implied, the terms of this Agreement shall govern. Without limiting the foregoing, no provision of any other agreement or understanding between the parties limiting the liability of the Business Associate to Covered Entity shall apply to the breach of any term, condition or covenant contained in this Agreement by Business Associate.
9. Headings. The headings of each section are inserted solely for purposes of convenience and shall not alter the meaning of this Agreement.
10. Governing Law. This Agreement shall be construed in accordance with and governed by the laws of the State of **<<ENTER THE APPROPRIATE STATE HERE>>.**

**IN WITNESS WHEREOF,** the parties have executed this Agreement effective upon the effective date set forth above.

“Covered Entity”

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

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

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

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Issue Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

“Business Associate”

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

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

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

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Issue Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_