If you conduct transactions in electronic form such as billing electronically or through a clearinghouse or use any electronic storage media, you are considered a "covered entity". Covered entities and business associates are required by The Health Insurance Portability and Accountability Act (HIPAA) to have a Business Associate Agreement that includes a Breach Notification, or to amend existing Business Associate Agreements that do not contain a Breach Notification.

The following Business Associate Agreement meets this requirement.

On the first page of the agreement, insert the date, your legal entity name on “covered entity” line and the name of business associate on “business associate” line.

Send agreement to Business Associate to complete signature section on last page and have them return to you. Then complete the Covered Entity section.

Keep the original in your compliance binder; send an executed copy to the Business Associate.

**\*\*\*\*\*DO NOT INCLUDE THIS PAGE AS PART OF THE AGREEMENT\*\*\*\*\***

**HIPAA Business Associate Agreement**

This Agreement dated as of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20XX is made by and between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Hereinafter “**Covered Entity**”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Hereinafter “**Business Associate**”).

**INTRODUCTION**

This Agreement governs the terms and conditions under which Business Associate will access personal health information belonging to patients of Covered Entity in performing services for, or on behalf of, Covered Entity. Specifically, this agreement governs the terms and conditions under which Business Associate will provide compliance consulting services to the Covered Entity.

**DEFINITIONS**

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR 160.103 and 164.501. For purposes of this section:

1. Individual. “Individual” shall have the same meaning as the term “Individual” in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
2. Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.
3. Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
4. Required By Law. “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR 164.501.
5. Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or their designee.

**OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE**

Business Associate agrees to:

1. Not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
2. Use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
3. Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
4. Report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement.
5. Ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
6. In the event that the Business Associate maintains PHI in a designated records set, Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524.
7. In the event that the Business Associate maintains Protected Health Information in a designated records set, Business Associate agrees to make any amendment(s) to Protected Health Information in a designated record set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity.
8. Make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule. In the event such a request comes directly from the Secretary, Business Associate agrees to notify Covered Entity immediately of such request.
9. Document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
10. Provide to Covered Entity or an Individual, in time and manner designated by Covered Entity, information collected in accordance with this section, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
11. Implementation of an Identity Theft Monitoring Policy and Procedure, to protect any patient information that may be breached by the Business Associate, under the Federal Trade Commission Regulations Red Flag Rules.
12. Obligation to report violations of patient privacy. Facilities will be required to report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information” both to the DHHS/OCR and to the affected patient (or the patient's representative) no later than five days after the unlawful or unauthorized access, use or disclosure has been detected.
* "Unauthorized" means inappropriate access, review or viewing of patient medical information without a direct need for medical diagnosis, treatment or other lawful use. This latter reference is broad enough to include HIPAA, as it operates in conjunction with State law.

**HITECH ACT REGULATIONS FOR BUSINESS ASSOCIATES**

The HITECH Act imposes on entities covered by the Health Insurance Portability and Accountability Act (HIPAA) and their business associates federal breach notification requirements when "unsecured" PHI is acquired by an unauthorized party. "Unsecured" means not secured through the use of a technology or methodology that renders the information "unusable, unreadable, or indecipherable" to unauthorized individuals. Information that has been "de-identified" is not subject to the breach notification requirements because such information is not protected under HIPAA.

In other words, the Act specifies circumstances under which PHI is no longer "unsecured" and accordingly avoids the HITECH Act's notification requirements. The guidance, however, provides that notice may be required to comply with other federal and state requirements.

The breach notification requirements will apply to PHI in any form. PHI may be vulnerable in any of the following commonly recognized data states:

* "Data in motion": Data that is moving through a wired or wireless network;
* "Data at rest": Data that resides in databases, files, or in storage;
* "Data in use": Data that is in the process of being created, maintained, updated, or destroyed; or
* "Data disposed": Data that has been discarded or recycled.

PHI in each of these data states, with the possible exception of "data in use," may be secured using one or more methods.

* Encryption, which will apply only to electronic information; and
* Destruction

Encryption of "data at rest" must satisfy NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Valid encryption processes for "data in motion" must comply with the requirements of Federal Information Processing Standards (FIPS) 140-2.

These include, as appropriate, standards described in NIST Special Publications 800-52; Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs; and may include others that are

FIPS 140-2 validated.

Destruction of PHI on paper, film, or other hard copy media must involve either shredding or otherwise destroying the PHI so that it cannot be read or reconstructed. PHI on electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved. Business Associate agrees to comply with all aspects of the HITECH Act.

**PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE**

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information, as follows:

1. On behalf of, Covered Entity, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.
2. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it 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, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

**OBLIGATIONS OF COVERED ENTITY**

Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

**PERMISSIBLE REQUESTS BY COVERED ENTITY**

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

**TERM AND TERMINATION**

1. Term. The obligations set forth in this section shall be effective as of the date the first protected health information is released to Business Associate pursuant to this Agreement, and shall terminate only when all of the Protected Health Information 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, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.
2. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation. Covered Entity may terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity.
3. Effect of Termination.

(i) Except as provided in paragraph (ii) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(ii) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

**Survival - The respective rights and obligations of Business Associate under this section shall survive the termination of this Agreement.**

**OWNERSHIP OF INFORMATION**

Covered Entity holds all right, title, and interest in and to the PHI and Business Associate does not hold and will not acquire by virtue of this Agreement or by virtue of providing goods or services to Covered Entity, any right, title, or interest in or to the PHI or any portion thereof.

**RIGHT TO INJUNCTIVE RELIEF**

Business Associate expressly acknowledges and agrees that the breach, or threatened breach, by it of any provision of this Agreement may cause Covered Entity to be irreparably harmed and that Covered Entity may not have an adequate remedy at law. Therefore, Business Associate agrees that upon such breach, or threatened breach, Covered Entity will be entitled to seek injunctive relief to prevent Business Associate from commencing or continuing any action constituting such breach without having to post a bond or other security and without having to prove the inadequacy of any other available remedies. Nothing in this paragraph will be deemed to limit or abridge any other remedy available to Covered Entity at law or in equity.

**MISCELLANEOUS**

1. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended, and for which Compliance is required.
2. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.
3. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

**COVERED ENTITY**

By:

Signature:

Title:

Date:

**BUSINESS ASSOCIATE**

By:

Signature:

Title:

Date: