**AMERICAN ACADEMY OF FAMILY PHYSICIANS’**

**SAMPLE BUSINESS ASSOCIATE AGREEMENT**(2013 Updated Security Rule Implementation)

**DISCLAIMER: The information provided in this document does not constitute legal or other professional advice, Nor is it a substitute for legal or other professional advice. YOU SHOULD CONSULT WITH ADVISORS FAMILIAR WITH YOUR STATES PRIVACY LAWS AND LAWS REGARDING THIRD PARTY BENEFICIARIES PRIOR TO USING THIS DOCUMENT.**

**Listing of Potential Business Associates**

A business associate is defined by the U.S. Department of Health and Human Services as “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 protected health information.” A business associate is also “a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.”

**Potential Business Associates:**

* Lawyers and legal counsel
* External auditors and accountants
* Professional translator services
* Answering services
* Consultants who require access to Protected Health Information (PHI), such as those who conduct coding reviews and audits
* Accreditation agencies
* Shredding and documentation storage companies (this includes cloud storage providers)
* Copy service (release of information)
* Medical transcription services (this includes contracting with an individual or company)
* Medical equipment service companies that service equipment containing PHI
* E-prescribing gateways
* Health information organizations
* Data processing firms
* Lockbox service
* Billing and coding service/agency
* Collection agency
* Practice management software vendors exposed to PHI
* Hardware maintenance service
* Other independent contractors who provide business and/or administrative services on-site and require access to PHI

**BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement, effective this \_\_\_\_\_\_ day of \_\_\_\_\_ , ("Effective Date"), is entered into by and between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(the "Business Associate") and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, a {physician licensed to practice medicine in the State of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **OR** a professional corporation organized under the laws of the State of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_} (the "Covered Entity") (each a "Party" and collectively the "Parties").

**WHEREAS**, Covered Entity and Business Associate are required to comply with the Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164, subparts A and E) ("Privacy Regulations") and for Security of electronic Protected Health Information ("PHI") (45 C.F.R. Part 164, subparts A and E ("Security Regulations"), as that term is defined in Section 164.501 of the Privacy Regulations, as promulgated by the U.S. Department of Health and Human Services ("HHS") pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), Title XIII of Division A and Title IV of Division B (the **"Health Information Technology for Economic and Clinical Health"** or **"HITECH Act"**) and other applicable laws; and,

**WHEREAS**, the Covered Entity has engaged the Business Associate to perform "Services" as defined below; and,

**WHEREAS,** in the performance of the Services, the Business Associate must use and/or disclose PHI received from or transmitted to the Covered Entity; and,

**WHEREAS**, the Parties are committed to complying with the Privacy and Security Regulations;

**NOW, THEREFORE**, in consideration of the mutual promises and covenants herein contained, the Parties enter into this Business Associate Agreement ("Agreement").

1. **SERVICES**

Business Associate provides {billing and collection, legal, accounting, health care business consulting, or specify other type of service} services for the Covered Entity ("Services"). In the course of providing the Services, the use and disclosure of PHI between the Parties may be necessary.

2. **PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION BY THE BUSINESS ASSOCIATE.**

Unless otherwise specified herein and provided that such uses or disclosures are permitted under state and Federal confidentiality laws, the Business Associate may:

1. Use the PHI in its possession to the extent necessary to perform the Services, subject to the limits set forth in 45 CFR §164.514 regarding limited data sets and 45 CFR §164.502(b) regarding the minimum necessary requirements;

1. Disclose to its employees, subcontractors, and agents the minimum amount of PHI in its possession necessary to perform the Services;

1. Use or disclose PHI in its possession as directed in writing by the Covered Entity;

1. Use the PHI in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of the Business Associate;

1. Disclose the PHI in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of the Business Associate, so long as the Business Associate represents, in writing, to the Covered Entity that (i) the disclosures are "required by law," as defined in Section 164.501 of the Privacy Regulations or (ii) the Business Associate has received written assurances from the third party regarding its confidential handling of such Protected Health Information as required in Section 164.504(e)(4) of the Privacy Regulations.

1. Aggregate the PHI in its possession with the PHI of other covered entities with which the Business Associate also acts in the capacity of a business associate so long as the purpose of such aggregation is to provide the Covered Entity with data analyses relating to the Health Care Operations of the Covered Entity. Under no circumstances may the Business Associate disclose PHI of Covered Entity to another covered entity unless such disclosure is explicitly authorized herein.

1. De-identify PHI so long as the de-identification complies with Section 164.514(b) of the Privacy Regulations, and the Covered Entity maintains the documentation required by Section 164.514(b) of the Privacy Regulations, which may be in the form of a written assurance from the Business Associate. Such de-identified information is not considered PHI under the Privacy Regulations.

3. **RESPONSIBILITIES OF THE BUSINESS ASSOCIATE WITH RESPECT TO PROTECTED HEALTH INFORMATION**

 The Business Associate further agrees to:

1. Use and/or disclose the Protected Health Information only as permitted or required by this Agreement or as otherwise required by law as defined in Section 164.501 of the Privacy Regulations and as modified by HITECH;

1. Use and disclose to its subcontractors, agents or other third parties, and request from the Covered Entity, only the minimum Protected Health Information necessary to perform the Services or other activities required or permitted hereunder;
2. 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;

1. Develop appropriate internal policies and procedures to ensure compliance with this Agreement and use other reasonable efforts to maintain the security of the PHI and to prevent unauthorized use and/or disclosure of such PHI, including but not limited to, compliance with Subpart C of 45 CFR Part 164 with respect to electronic PHI;
2. To the extent the Business Associate is to carry out one or more of the 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);

1. Notify the Covered Entity's designated Privacy Officer, in writing, of any use and/or disclosure, and any other security incident of which it becomes aware, of the PHI not permitted or required hereunder within three (3) days of the Business Associate's discovery of such unauthorized use and/or disclosure or other security incident;

1. Develop and implement policies and procedures for mitigating, to the greatest extent possible, any negative or unintended effects caused by the improper use and/or disclosure of PHI that the Business Associate reports to the Covered Entity;
2. 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;
3. Make any amendments 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 the Covered Entity's obligations under 45 CFR § 164.526;

1. Provide the Covered Entity with all information the Covered Entity requests, in writing, to respond to a request by an individual for an accounting of the disclosures of the individual's PHI as permitted in Section 164.528 of the Privacy Regulations within thirty (30) days of receiving the request;

1. Upon two (2) days' written notice, allow access by the Covered Entity all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI at Business Associate's offices so that the Covered Entity may determine the Business Associate's compliance with the terms of this Agreement;

1. Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI as requested by the Secretary of HHS for determining the Covered Entity's compliance with the Privacy and Security Regulations, subject to attorney-client and other applicable legal privileges;

1. Require all of its subcontractors and agents that receive or use, or have access to, PHI to agree, in writing, to adhere to the same restrictions and conditions that apply to the Business Associate pursuant to this Agreement;

1. Return to the Covered Entity or destroy, within thirty (30) days of the termination of this Agreement, the PHI in its possession and retain no copies (which for purposes of this Agreement shall mean destroy all back-up tapes); and
2. Notify the Covered Entity within twenty (20) days of the discovery of any breaches of unsecured PHI as required by 45 CFR § 164.410.

4. **RESPONSIBILITIES OF THE COVERED ENTITY WITH RESPECT TO PROTECTED HEALTH INFORMATION**

 The Covered Entity hereby agrees:

1. To advise the Business Associate, in writing, of any arrangements of the Covered Entity under the Privacy Regulations that may impact the use and/or disclosure of PHI by the Business Associate under this Agreement;

1. To provide the Business Associate with a copy of the Covered Entity's current Notice of Privacy Practices ("Notice") required by Section 164.520 of the Privacy Regulations and to of provide revised copies of the Notice, should the Notice be amended in any way;
2. To advise the Business Associate, in writing, of any revocation of any consent or authorization of any individual and of any other change in any arrangement affecting the use and or disclosure of PHI to which the Covered Entity has agreed, including, but not limited to, restrictions on use and/or disclosure of PHI pursuant to Section 164.522 of the Privacy Regulations;

1. {Use only if Services involve marketing or fundraising} to inform the Business Associate of any individual who elects to opt-out of any marketing and/or fundraising activities of the Covered Entity;

1. That Business Associate may make any use and/or disclosure of Protected Health Information as permitted in Section 164.512 with the prior written consent of the Covered Entity.
2. **REPRESENTATIONS AND WARRANTIES OF BOTH PARTIES**

Each Party represents and warrants to the other Party that:

1. It is duly organized, validly existing, and in good standing under the laws of the state in which it is organized or licensed;

1. It has the power to enter into this Agreement and to perform its duties and obligations hereunder;

1. All necessary corporate or other actions have been taken to authorize the execution of the Agreement and the performance of its duties and obligations;

1. Neither the execution of this Agreement nor the performance of its duties and obligations hereunder will violate any provision of any other agreement, license, corporate charter or bylaws of the Party;

1. it will not enter into nor perform pursuant to any agreement that would violate or interfere with this Agreement;

1. It is not currently the subject of a voluntary or involuntary petition in bankruptcy, does not currently contemplate filing any such voluntary petition, and is not aware of any claim for the filing of an involuntary petition;

1. Neither the Party, nor any of its shareholders, members, directors, officers, agents, employees or contractors have been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any Federal or state healthcare program, including but not limited to Medicare or Medicaid or have been convicted, under Federal or state law of a criminal offense;

1. All of its employees, agents, representatives and contractors whose services may use or disclose PHI on behalf of that Party have been or shall be informed of the terms of this Agreement;

1. All of its employees, agents, representatives and contractors who may use or disclose PHI on behalf of that Party are under a sufficient legal duty to the respective Party, either by contract or otherwise, to enable the Party to fully comply with all provisions of this Agreement.

**Each Party further agrees to notify the other Party immediately after the Party becomes aware that any of the foregoing representation and warranties may be inaccurate or may become incorrect.**

6. **TERM AND TERMINATION**

This Agreement shall become effective on the Effective Date and shall continue unless and until either Party provides ninety (90) days' written notice of its intention to terminate the Agreement to the other, or the Agreement is otherwise terminated hereunder.

If the Covered Entity makes the determination that the Business Associate has breached a material term of this Agreement, then at the sole discretion of the Covered Entity, it may either terminate this Agreement immediately upon written notice to the Business Associate or provide the Business Associate with written notice of the material breach and allow the Business Associate fifteen (15) days to cure such breach upon mutually agreeable terms; provided, however, that if an agreement regarding a satisfactory cure is not achieved within the fifteen (15) days, the Covered Entity may immediately terminate this Agreement upon written notice to the Business Partner.

**This Agreement will automatically terminate without further notice if the Business Associate no longer provides Services for the Covered Entity**.

 Upon termination of this Agreement for any reason, the Business Associate shall:

1. Recover any PHI in the possession of its agents or contractors;

1. At the option of the Covered Entity and if feasible, either return all PHI in its possession to Covered Entity or destroy all PHI in its possession (Business Associate shall retain no copies of PHI).

If it is determined by the Business Associate that it is not feasible to return or destroy any or all of the PHI, the Business Associate must notify the Covered Entity of the specific reasons in writing. The Business Associate must continue to honor all protections, limitations, and restrictions herein with regard to the Business Associate's use and/or disclosure of PHI so retained and to limit any further uses and/or disclosures to the specific purposes that render the return or destruction of the PHI not feasible.

Further, the Business Associate shall provide written notice to the Covered Entity if it is unable, because it is not feasible, to obtain any or the entire PHI in the possession of an agent or contractor. The Business Associate shall require the agent or contractor to honor any and all protections, limitations, and restrictions herein with regard to the agent's or contractor's use and/or disclosure of any PHI so retained and to limit any further uses and/or disclosures to the specific purposes that render the return or destruction of the PHI not feasible.

7. **INDEMNIFICATION**

The Business Associate hereby agrees to indemnify, defend, and hold harmless the Covered Entity and its shareholders, directors, officers, partners, members, employees, agents, and/or contractors (collectively "Indemnified Party") against any losses, liabilities, fines, penalties, costs, or expenses (including reasonable attorneys' fees) which may be imposed upon the Covered Entity by reason of any suit, claim, action, proceeding, or demand by any third party which results from the Business Associate's breach of this Agreement or from any negligence or wrongful acts or omissions, including failure to comply with the terms and requirements of the Privacy or Security Regulations, by the Business Associate, its shareholders, directors, officers, partners, members, employees, agents, and/or contractors. This obligation of the Business Associate to indemnify the Covered Entity shall survive the termination of this Agreement for any reason.

8. **GENERAL PROVISIONS**

1. If the Covered Entity operates under a Joint Notice of Privacy Practices ("Joint Notice"), as defined in the Privacy Regulations, then this Agreement shall apply to all entities covered by the Joint Notice as if each such entity were the Covered Entity.

1. If the Business Associate is also a covered entity, as defined in the Privacy Regulations, then that covered entity may designate a health care component, as defined in Section 164.504 of the Privacy Regulations, which shall be considered the Business Associate hereunder.

1. This Agreement may not be modified or amended except in a writing signed by both Parties.

1. No waiver of any provision of this Agreement by either Party shall constitute a general waiver for future purposes.

1. This Agreement may not be assigned by the Business Associate without written approval of the Covered Entity. The Covered Entity may assign this Agreement upon written notice to the Business Associate.

1. This Agreement shall inure to the benefit of and be binding upon the Parties, their respective successors or assigns.

1. The invalidity or unenforceability of any particular provision of this Agreement shall not affect the other provisions hereof, and this Agreement shall be construed in all respects as though such invalid or unenforceable provision was omitted.

1. The Provisions of this Agreement shall survive termination of this Agreement to the extent necessary to effectuate their terms or indefinitely with respect to the use and disclosure of PHI.

1. Any notices to be given hereunder shall be given via U.S. Mail, return receipt requested, or by a recognized commercial express courier, as follows:

 If to Business Associate, to:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Attention: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Fax: ( ) \_\_\_\_\_\_\_\_\_\_\_\_\_\_with a copy (which shall not constitute notice) to: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Each Party named above may change its address and/or the name of its representative by providing notice thereof in the manner provided above. If personally delivered, such notice shall be effective upon delivery. If mailed or delivered by private carrier in accordance with this Section, such notice shall be effective as of the date indicated on the return receipt whether or not such notice is accepted by the addressee.

1. This Agreement shall be construed according to the laws of the State of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ applicable to contracts formed and wholly performed within that State. The Parties further agree that should a cause of action arise under any Federal law, the suit shall be brought in the Federal District Court where the Covered Entity is located.

1. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

1. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND OR NATURE, WHETHER SUCH LIABILITY IS ASSERTED ON LAWS.

**IN WITNESS WHEREOF**, the parties hereto have duly executed this agreement to be effective as of [effective date of the agreement].

Physician Practice ***[Insert Practice Name and Address]***

Name: .

Title: ..

Date: .

Business Associate ***[Insert Company/Individual Name and Address]***

Name: .

Title: ..

Date: .