

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“**Agreement**”), dated _____, 200__, is entered into by and between [Insert Name of Practice] (“**Covered Entity**”) and [Insert Name of Vendor] (the “**Business Associate**”) (each a “**Party**” and collectively the “**Parties**”).

Recitals

WHEREAS, Covered Entity has engaged Business Associate to perform services and/or provide goods (“**Service Agreement**”);

WHEREAS, Covered Entity possesses Individually Identifiable Health Information that is protected under HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations and the HITECH Standards and is permitted to use or disclose such information only in accordance with such laws and regulations;

WHEREAS, Business Associate may receive such information from Covered Entity, or create and receive such information on behalf of Covered Entity, in order to perform in accordance with the Service Agreement; and

WHEREAS, Covered Entity wishes to ensure that Business Associate will appropriately safeguard Individually Identifiable Health Information;

NOW, THEREFORE, for good and valuable consideration, the sufficiency of which we hereby acknowledge, the Parties agree as follows:

Section 1 **Definitions**

- 1.1 Terms used but not otherwise defined in this Agreement shall have the same meaning as the meaning ascribed to those terms in the Health Information Portability and Accountability Act of 1996, as codified at 42 U.S.C. § 1320d (“**HIPAA**”), the Health Information Technology Act of 2009, as codified at 42 U.S.C.A. prec. § 17901 (“**HITECH**”), and any current and future regulations promulgated under HIPAA or HITECH.
- 1.2 “**Breach**” shall mean the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted under 45 C.F.R. Part 164, Subpart E (the “HIPAA Privacy Regulations”) which compromises the security or privacy of the Protected Health Information. “Breach” shall not include:
 - (a) Any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of Covered Entity or Business Associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Regulations; or

- (b) Any inadvertent disclosure by a person who is authorized to access Protected Health Information at Covered Entity or Business Associate to another person authorized to access Protected Health Information at Covered Entity or Business Associate, respectively, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations; or
 - (c) A disclosure of Protected Health Information where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- 1.3 **“Electronic Protected Health Information”** or **“Electronic PHI”** means Protected Health Information that is transmitted by or maintained in electronic media as defined in the HIPAA Security Regulations.
- 1.4 **“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).
- 1.5 **“HIPAA Privacy Regulations”** shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.
- 1.6 **“HIPAA Security Regulations”** shall mean the Standards for Security of Individually Identifiable Health Information at 45 C.F.R. part 160 and subparts A and C of part 164.
- 1.7 **“HITECH Standards”** means the privacy, security and security Breach notification provisions applicable to a Business Associate under Subtitle D of HITECH and any regulations promulgated thereunder.
- 1.8 **“Individually Identifiable Health Information”** means information that is a subset of health information, including demographic information collected from an individual, and;
 - (a) is created or received by a health care provider, health plan, employer or health care clearinghouse; and
 - (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
 - (i) that identifies the individual; or
 - (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- 1.9 **“Protected Health Information”** (or “PHI”) shall have the same meaning as the term “protected health information” in 45 CFR 160.103 (as amended by the HITECH Act), limited to the information created or received by Business Associate from or on behalf of Covered Entity including, but not limited to Electronic PHI.
- 1.10 **“Required By Law”** shall have the same meaning as the term “required by law” in 45 CFR 164.5011.11.
- 1.11 **“Secretary”** shall mean the Secretary of the Department of Health and Human Services or his designee.

- 1.12 **“Unsecured Protected Health Information”** shall mean PHI that is not secured through the use of technology or methodology specified by the Secretary in regulations or as otherwise defined in section 13402(h) of HITECH.

Section 2
Obligations and Activities of Business Associate

In order that Covered Entity and Business Associate may achieve and maintain compliance with the requirements of HIPAA and HITECH, Business Associate agrees:

- 2.1 **Not to Use or Disclose PHI Unless Permitted.** Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law. Business Associate may 1) use and disclose PHI to perform its obligations applicable to the Service Agreement; (2) use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities; (3) disclose PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities, if such disclosure is required by law or if Business Associate obtains reasonable assurances from the recipient that the recipient will keep the PHI confidential, use or further disclose the PHI only as required by law or for the purpose for which it was disclosed to the recipient, and notify Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached; (4) use PHI to provide data aggregation services relating to the health care operations of Covered Entity; (5) use or disclose PHI to report violations of the law to law enforcement; and (6) use PHI to create de-identified information consistent with the standards set forth at 45 CFR §164.514. Business Associate will not sell PHI or use or disclose PHI for purposes of marketing, as defined and proscribed in the Regulations.
- 2.2 **Safeguards.** Business Associate agrees to use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- 2.3 **Mitigation.** Business Associate agrees to 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.
- 2.4 **Notice of Use or Disclosure, Security Incident or Breach.** Business Associate agrees to notify the designated Privacy Official of the Covered Entity of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident (as defined in 45 C.F.R. section 164.304) involving Electronic PHI, and any Breach of Unsecured Protected Health Information within five (5) business days.
- (a) Business Associate shall provide the following information to Covered Entity within ten (10) business days of discovery of a Breach except when despite all reasonable efforts by Business Associate to obtain the information required, circumstances beyond the control of the Business Associate necessitate additional time. Under such circumstances Business Associate shall provide to Covered Entity the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a Breach:
- (i) the date of the Breach;

- (ii) the date of the discovery of the Breach;
- (iii) a description of the types of unsecured PHI that were involved;
- (iv) identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
- (v) any other details necessary to complete an assessment of the risk of harm to the Individual.

- (b) Covered Entity will be responsible to provide notification to Individuals whose unsecured PHI has been disclosed, as well as the Secretary and the media, as required by Sec. 13402 of the HITECH Act, 42 U.S.C.A. § 17932.
- (c) Business Associate agrees to pay actual costs for notification for any associated mitigation costs incurred by Covered Entity, such as credit monitoring, if Covered Entity determines that the Breach is significant enough to warrant such measures.
- (d) Business Associate agrees to establish procedures to investigate the Breach, mitigate losses, and protect against any future Breaches, and to provide a description of these procedures and the specific findings of the investigation to Covered Entity in the time and manner reasonably requested by Covered Entity.
- (e) The Parties agree that this section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. For purposes of this Agreement, "Unsuccessful Security Incidents" include activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of Electronic PHI.

- 2.5 **Compliance of Agents.** Business Associate agrees to 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.
- 2.6 **Access.** 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.
- 2.7 **Amendments.** Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity.
- 2.8 **Disclosure of Practices, Books, and Records.** Business Associate agrees to 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 in determining Covered Entity's compliance with the HIPPA Privacy Regulations.

- 2.9 **Accounting.** To provide documentation regarding any disclosures by Business Associate that would have to be included in an accounting of disclosures to an Individual under 45 CFR 164.528 (including without limitation a disclosure permitted under 45 CFR 164.512) and under HITECH, within a reasonable amount of time of receipt of a request from Covered Entity.
- 2.10 **Security of Electronic Protected Health Information.** Business Associate agrees to (1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of the Covered Entity; (2) ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (3) report to the Covered Entity any security incident of which it becomes aware.
- 2.11 **Minimum Necessary.** To limit its uses and disclosures of, and requests for, PHI (a) when practical, to the information making up a Limited Data Set; and (b) in all other cases subject to the requirements of 45 CFR 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.
- 2.12 **Compliance with HITECH Standards.** Notwithstanding any other provision in this Agreement, no later than February 17, 2010, unless a separate effective date is specified by law or this Agreement for a particular requirement (in which case the separate effective date shall be the effective date for that particular requirement), Business Associate shall comply with the HITECH Standards, including, but not limited to: (1) compliance with the requirements regarding minimum necessary under HITECH section 13405(b); (2) requests for restrictions on use or disclosure to health plans for payment or health care operations purposes when the provider has been paid out of pocket in full consistent with HITECH section 13405(a); (3) the prohibition of sale of PHI without authorization unless an exception under HITECH section 13405(d) applies; (4) the prohibition on receiving remuneration for certain communications that fall within the exceptions to the definition of marketing under 45 C.F.R. section 164.501 unless permitted by this Agreement and section 13406 of HITECH; (5) the requirements relating to the provision of access to certain information in electronic access under HITECH section 13405(e); (6) compliance with each of the Standards and Implementation Specifications of 45 C.F.R. section 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards) and 164.316 (Policies and Procedures and Documentation Requirements); and (7) the requirements regarding accounting of certain disclosures of PHI maintained in an Electronic Health Record under HITECH section 13405(c).
- 2.13 **Indemnification.** Business Associate agrees to indemnify, insure, defend and hold harmless Covered Entity and Covered Entity's employees, directors, officers, subcontractors, agents, or members of its workforce, each of the foregoing hereinafter referred to as an "**indemnified party**," against all actual and direct losses suffered by the indemnified party and all liability to third parties arising from or in connection with any breach of this Agreement or of any warranty hereunder or from any negligence, wrongful acts, or omissions, including the failure to perform its obligations under HIPAA, as well as the additional obligations under HITECH, by Business Associate or its employees, directors, officers, subcontractors, agents, or members of its workforce. This includes, but is not limited to, expenses associated with notification to individuals and/or the media

in the event of a breach of Protected Health Information held by Business Associate. Accordingly, on demand, Business Associate shall reimburse any indemnified party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any indemnified party by reason of any suit, claim, action, proceeding or demand by any third party which results from the indemnifying party's breach hereunder. The provisions of this paragraph shall survive the expiration or termination of this Agreement for any reason.

Section 3

Permitted Uses and Disclosures by Business Associate **General Use and Disclosure Provisions**

- 3.1 **Permitted Uses and Disclosures.** Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity applicable to the Service Agreement(s) between the Parties provided that such use or disclosure would not violate HIPAA or HITECH if done by Covered Entity.

Section 4

Obligations of Covered Entity

- 4.1 **Notice of Privacy Practices 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.
- 4.2 **Restriction in Use of PHI.** Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed.

Section 5

Term and Termination

- 5.1 **Term.** The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate 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.
- 5.2 **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 and any other Agreement between Covered Entity and Business Associate if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity. In addition, Covered Entity may immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.
- 5.3 **Effect of Termination.**
- (a) Except as provided in section 5.2, 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.

(b) 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.

Section 6
Miscellaneous

- 6.1 **Regulatory References.** A reference in this Agreement to a section in HIPAA or HITECH means the section as in effect or as amended, and for which compliance is required.
- 6.2 **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 HIPAA or HITECH and any applicable regulations in regard to such laws.
- 6.3 **Survival.** The respective rights and obligations of Business Associate shall survive the termination of this Agreement.
- 6.4 **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA or HITECH or any applicable regulations in regard to such laws.

[Insert Name of Business Associate]

[Insert Name of Covered Entity]

By: _____
Signature
[Insert Title of Signer]

By: _____
Signature
[Insert Title of Signer]