

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into by and between _____, hereafter referred to as the Covered Entity ("CE") and _____, hereafter referred to as the Business Associate ("Associate"), and is effective as of _____, (the "Agreement Effective Date").

RECITALS

WHEREAS, Business Associate and CE have entered into an Agreement under which Business Associate performs or assists CE with functions or activities involving the use or disclosure of Individually Identifiable Protected Health Information (PHI) or electronic PHI;

WHEREAS, CE and Business Associate desire to comply with the requirements of regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which privacy regulations are codified at 45 C.F.R. parts 160 and 164 and which security regulations are codified at 45 C.F.R. part 160, 162 and 164, as such regulations may be amended from time to time (collectively referred to herein as the "HIPAA Standards");

WHEREAS, CE and Business Associate acknowledge and agree that capitalized terms used, but not otherwise defined, herein are as defined in the HIPAA Standards;

WHEREAS, the HIPAA Standards require that CE obtain satisfactory assurances that Business Associate will appropriately safeguard the PHI used or disclosed by Business Associate in the course of performing services pursuant to the Agreement.

DEFINITIONS

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, 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.
- (b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.
- (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

- (a) Compliance with Applicable Laws and Regulations. Business Associate shall, in the performance of its duties under this Business Associate Agreement, comply with all applicable state and federal laws, regulations, and rules including, without limitation, HIPAA's Security Rule and the HITECH Act's Privacy Provisions. Pursuant to this obligation, Business Associate must, at a minimum, perform a risk analysis, periodically reassess and update security protections and implement reasonable and appropriate security policies and procedures. Additionally, when carrying out a HIPAA obligation of CE, Business Associate must comply with the HIPAA Privacy Rule to the same extent as CE would be required to.
- (b) Nondisclosure. Business Associate shall not use or disclose PHI other than as permitted or required by the Agreement or as required by law. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by CE. Additionally, to the extent Business Associate is to carry out one or more of CE's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate must comply with the requirements of Subpart E that apply to CE in the performance of such obligation(s), except for the specific uses and disclosures set forth in this Agreement.
- (c) Safeguards. Business Associate shall 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.

Business Associate shall implement and maintain safeguards as necessary to ensure that all PHI, including without limitation any electronic protected health information, is used or disclosed only as authorized under the HIPAA Standards and this Business Associate Agreement. Business Associate agrees to assess potential risks and vulnerabilities to PHI in its possession and develop, implement, and maintain the administrative, physical, and technical safeguards required by the HIPAA Standards that protect the confidentiality, availability, and integrity of the PHI that Business Associate creates, receives, maintains, or transmits on behalf of CE. These measures must be documented and kept current, and must include, at a minimum, those measures that fulfill the requirements outlined in the HIPAA Standards. Business Associate also agrees to implement policies and procedures that address Business Associate's compliance with applicable HIPAA Standards and its efforts to detect, prevent, and mitigate the risks of identity theft resulting from the improper use and/or disclosure of an Individual's information.

- (d) Notification of Breach. Business Associate shall report to CE any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, including suspected breaches of unsecured PHI as required at 45 CFR 164.410, or an Individual's information not provided for by this Business Associate Agreement, including without limitation, any breach of PHI, unsecured PHI, or an Individual's information, and any Security Incident involving the PHI or an Individual's information of which Business Associate becomes aware, within twenty-four (24) hours of discovery of the suspected or actual breach of security, intrusion, or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. A breach shall be considered "discovered" as of the first day on which the breach is known, or reasonably should have been known, to Business Associate or any employee, officer, or agent of Business Associate, other than the individual committing the breach. Such notice shall identify the nature of the breach, including (i) a description of what happened; (ii) the date of the breach and (iii) specific elements of PHI that were subject to the breach.

Business Associate shall take any action necessary or requested by CE to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a security incident or use or disclosure of PHI, unsecured PHI, or an Individual's information by Business Associate in violation of the requirements of this Business Associate Agreement. In the event of a breach of PHI or unsecured PHI, Business Associate's notice to CE of such breach shall include, to the extent possible, the identification of each individual whose PHI has been, or is reasonably believed by Business Associate, to have been, accessed, acquired, or disclosed during such breach. Business Associate shall also provide CE any other available information that CE is required to include in the notification to the Individual, even if such information becomes available after notification to the Individual, or take any action necessary as requested by CE to assist CE in complying with any applicable breach notification requirements.

Business Associate shall further take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations. Business Associate shall also report a pattern of material breach of PHI by a subcontractor, pursuant to 45 CFR 164.504 (e)(1)(ii).

Business Associate agrees to reasonably cooperate and coordinate with CE in the investigation of any violation of the requirements of this Agreement and/or any security incident or breach. Business Associate shall also reasonably cooperate and coordinate with CE in the preparation of any reports or notices to the individual, a regulatory body, or any third party required under HIPAA, the HITECH Act, or any other Federal or State laws, rules or regulations, provided that any such reports or notices shall be subject to the prior written approval of CE. Notwithstanding anything in this section to the contrary, Business Associate may delay notification of a breach of a Unsecured PHI to CE in the event Business Associate is instructed to do so by a law enforcement official.

- (e) Subcontractors. Business Associate shall, 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. Business Associate acknowledges that if it or any of its subcontractors, regardless of any business associate agreement between Business Associate and such subcontractor, violates

any of the requirements provided under this Business Associate Agreement, Business Associate will be subject to the same civil and criminal penalties that a Covered Entity would be subject to if such Covered Entity violated the same requirements.

- (f) Availability of Information to the Department of Health and Human Services (HHS). Business Associate shall 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 Business Associate on behalf of, CE for purposes of HHS determining CE's compliance with the HIPAA Privacy Rule.
- (g) Availability of Information to Individuals and CE. Business Associate shall make available PHI in a designated record set to CE or to an individual designated by CE as necessary to satisfy CE's obligations under 45 CFR 164.524. Business Associate shall also make available to CE such information as CE may require to fulfill CE's obligations to provide access to, provide a copy of, and account for disclosures with respect to PHI pursuant to the HIPAA Laws as necessary to satisfy CE's obligations under 45 CFR 164.524 and 45 CFR 164.528.
- (h) Amendment to PHI. Business Associate shall make any amendment(s) to PHI in a designated record set as directed or agreed to by CE pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy CE's obligations under 45 CFR 164.526. Business Associate shall incorporate any amendments to the information in the designated record set within three (3) business days. Where CE receives a request for inspection and/or copying of PHI, which is created and maintained by Business Associate, CE's Privacy Officer will pass along the request to Business Associate, and Business Associate shall be responsible for fulfilling the request as appropriate.
- (i) Accounting of Disclosures. Business Associate shall maintain and make available such disclosures of PHI and information related to such disclosures as would be required for CE or Business Associate to respond to a request by an Individual for an accounting of disclosures of PHI to satisfy CE's obligations under 45 CFR 164.528. Business Associate shall provide the accounting of disclosures within five (5) business days.
- (j) Responding to an Individual's Request for Accounting of Disclosures. Business Associate shall provide to CE, in a time and manner designated by CE, information pertaining to disclosures of PHI by Business Associate to permit CE to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528. In the event that Business Associate receives a direct request from an Individual for an accounting of disclosures of PHI made by Business Associate during the six (6) years prior to the date of such request, Business Associate agrees to provide the Individual with such an accounting in accordance with 45 C.F.R. §164.528.
- (k) Restrictions on Certain Disclosures of PHI. If an Individual requests that Business Associate restrict the disclosure of the Individual's PHI to carry out treatment, payment, or health care operations, Business Associate agrees that it will comply with the requested restriction if, except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment), and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full by the individual or by someone on his or her behalf (other than the health plan) for said item or service.
- (l) To the extent Business Associate is to carry out one or more of CE's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to CE in the performance of such obligation(s).
- (m) Internal Practices. Business Associate shall make its internal practices, books, records, and compliance reports relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, CE available to CE or the Secretary, in a time and manner designated by CE or the Secretary, for purposes of the Secretary determining CE's or Business Associate's compliance with the HIPAA Standards.

PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

- (a) Business associate may only use or disclose PHI in only accordance with the specifications set forth in this Agreement and in accordance with 45 CFR 164.502 (e) (1) (iii) and 45 CFR 164.38 (b) (2), which can be modified at any time if agreed upon by both parties.
- (b) Business Associate is expressly prohibited from de-identifying PHI as defined in 45 CFR 164.514.
- (c) Business Associate may use or disclose PHI as required by law.
- (d) Except as otherwise permitted by the HIPAA Standards, when using or disclosing PHI or

responding to a request for PHI, Business Associate must limit such PHI, to the extent practicable, to a Limited Data Set, or if more information than a Limited Data Set is required, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request consistent with CE's minimum necessary policies and procedures.

- (e) Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by CE, except for the specific uses and disclosures set forth below.
- (f) Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
- (g) Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of 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.
- (h) Except as otherwise permitted by the HIPAA Standards, Business Associate agrees that it will not directly or indirectly receive remuneration in exchange for any PHI unless CE has obtained from an Individual a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the Individual's PHI.
- (i) Except as otherwise permitted by the HIPAA Standards, Business Associate agrees that it will not use or disclose PHI in connection with any fundraising and/or marketing communication for or on behalf of CE unless CE has obtained a valid authorization from each Individual who will be a recipient of any such communication.
- (j) Business Associate shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement, the HITECH Act or HIPAA.
- (k) Business Associate may provide "data aggregation" services relating to the health care operations of CE. For purposes of this Section, "data aggregation" means, with respect to CE's PHI, the combining of such PHI by Business Associate with the PHI received by Business Associate in its capacity as a Business Associate of another CE to permit data analyses that relate to the health care operations of the respective Covered Entities.

OBLIGATIONS OF COVERED ENTITY

- (a) CE shall provide Business Associate with the Notice of Privacy Practices that CE produces in accordance with 45 C.F.R. §164.520, as well as any changes to such Notice and the Business Associate shall comply with such Notice of Privacy Practices.
- (b) CE shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.
- (c) CE shall notify Business Associate of any restriction to the use or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. §164.522.
- (d) CE shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Standards if done by CE.
- (e) CE shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy, and security of PHI transmitted to Business Associate pursuant to this Agreement, in accordance with the standards and requirements of the HIPAA Laws, until such PHI is received by Business Associate.

TERM AND TERMINATION

- (a) Term. The Term of this Agreement shall be effective as of _____ and shall terminate (1) when all of the PHI provided by CE to Business Associate, or created or received by Business Associate on behalf of CE, is destroyed or returned to CE, or, if it is infeasible to return or destroy the PHI, protections are extended to such information, in accordance with the termination provisions in this Section, or (2) on the date CE 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 CE if CE determines Business Associate has violated a material term of the Agreement. CE may, at its discretion, allow Business Associate to cure a violation or breach of the contract before termination for cause within a timeframe specified by CE. If Business Associate does not cure the breach or end the violation within the timeframe specified by CE, or if cure is not possible, then CE shall terminate this Agreement forthwith. If termination of this Agreement is not

feasible, CE shall report Business Associate's breach or violation to the Secretary of the Department of Health and Human Services.

Material Breach shall include Business Associate's improper use or disclosure of PHI and any changes or any diminution of Business Associate's reported security procedures or safeguards that render any or all of Business Associate's safeguards unsatisfactory to CE, in CE's sole discretion.

Judicial or Administrative Proceedings – Either party may terminate this Agreement, effective immediately, if (i) the other party is named as a defendant in a criminal proceeding for a violation of the HIPAA Laws or (ii) a finding or stipulation that the other party has violated any standard or requirement of the HIPAA Laws or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

- (c) Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from CE, or created, maintained, or received by Business Associate on behalf of CE, 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 CE or, if agreed to by CE, destroy, the remaining PHI that Business Associate still maintains in any form;
In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to CE notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.
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 above under "Permitted Uses and Disclosures By Business Associate" which applied prior to termination;
5. Return to CE or, if agreed to by CE, 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;
6. Ensure the destruction of PHI created, received, or maintained by Business Associate's subcontractors.

The parties hereto understand and agree that the terms of this Agreement are reasonable and necessary to protect the interests of CE and the Business Associate. The parties further agree that CE would suffer irreparable harm if the Business Associate breached this Agreement. Thus, in addition to any other rights or remedies, all of which shall be deemed cumulative, CE shall be entitled to obtain injunctive relief to enforce the terms of this Agreement.

MISCELLANEOUS

- (a) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.
- (b) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
- (c) 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.
- (d) Interpretation. This Agreement shall be interpreted as broadly as necessary to implement and comply with the Privacy and Security laws, rules and regulations as well as applicable state laws. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Standards.
- (e) No Private Cause of Action. This Agreement is not intended to and does not create a private cause of action by any individual, other than the parties to this Agreement, as a result of any claim arising out of the breach of this Agreement, the HIPAA Standards, or other state or federal law or regulation relating to privacy or confidentiality.

- (f) Application of State Law. Where any applicable provision of state law relates to the privacy of health information and is not preempted by HIPAA, as determined by application of the HIPAA Standards, the parties shall comply with the applicable provisions of state law.
- (g) Severability. If any provision of this Agreement shall be declared invalid or illegal for any reason whatsoever, then notwithstanding such invalidity or illegality, the remaining terms and provisions of this Agreement shall remain in full force and effect in the same manner as if the invalid or illegal provision had not been contained herein, and such invalid, unenforceable, or illegal provision shall be valid, enforceable, and legal to the maximum extent permitted by law.
- (h) Governing Law. This Agreement shall be interpreted, construed and governed according to the laws of the state in which CE maintains its principal place of business. The parties agree that venue shall lie in federal and state courts in the state in which CE maintains its principal place of business, without regard to its conflicts of law principles, regarding any and all disputes arising from this Agreement.
- (i) Notices. Any notice or other communication given pursuant to this Agreement must be in writing and (i) delivered personally, (ii) delivered by overnight express, or (iii) sent by registered or certified mail, postage prepaid, to the address set forth above and shall be considered given upon delivery.
- (j) Indemnification. Without limitation to any indemnification obligation that Business Associate may have under the Agreement, Business Associate shall indemnify, hold harmless and defend CE (including CE's Board of Directors, individually and collectively, and its officers, owners, members, employees, agents, and other representatives, individually and collectively) from and against any and all claims, losses, liabilities, costs, and other expenses resulting from, or relating to, the acts or omissions of Business Associate, its employees, agents, and/or subcontractors, in connection with any use or disclosure of PHI, Unsecured PHI or an Individual's information not provided for by this Agreement, including without limitation any Breach of PHI, Unsecured PHI, or an Individual's information, or any expenses incurred by CE in providing required breach notifications.
- (k) Disclaimer. CE makes no warranty or representation that compliance by Business Associate with this Agreement, the HIPAA Laws will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.
- (l) Certification. To the extent that CE determines that such examination is necessary to comply with CE's legal obligations pursuant to the HIPAA Laws relating to certification of its security practices, CE or its authorized agents or contractors, may, at CE's expense, examine Business Associate's facilities systems, procedures, and records as may be necessary for such agents or contractors to certify to CE the extent to which Business Associate's security safeguards comply with the HIPAA Laws or this Agreement. Business Associate may elect to retain an independent third-party to conduct a privacy audit in lieu of inspection by CE or its authorized agents or contractors. Business Associate's selection of an independent third-party is subject to CE's approval. CE and Business Associate agree to equally share the expense incurred in hiring such independent third-party.
- (m) Agreement. CE and Business Associate agree that both CE and Business Associate are required to comply as "covered entities" under the HIPAA Laws and the obligations of this Agreement are intended to apply mutually to both CE and Business Associate.
- (n) Agreement to Comply with Law. The parties acknowledge that applicable state and federal laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of the HIPAA Laws and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that CE must receive satisfactory written assurance from Associate that Associate will adequately safeguard all PHI that it receives or creates pursuant to this Agreement. Upon CE's request, Business Associate agrees to promptly to enter into negotiations with CE concerning the terms of an amendment to this Agreement embodying written assurances consistent with the standards and requirements of the HIPAA Laws or other applicable laws. CE may terminate this Agreement upon thirty (30) days written notice in the event that (1) Business Associate does not promptly

enter into negotiations to amend this Agreement when requested by CE pursuant to this Section; or (2) Business Associate does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of the HIPAA Laws.

- (o) Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself, and any subcontractors, employees, or agents assisting Business Associate in the performance of its obligations under this Agreement, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers, or employees based upon claimed violation of the HIPAA Laws or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee, or agent is a named adverse party.
- (p) No Third-Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CE, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.
- (q) Effect on Agreement. Except as specifically required to implement the purposes of this Agreement, or to the extent inconsistent with this Agreement, all other terms of the Agreement shall remain in force and effect.
- (r) Integration and Interpretation. This Agreement contains the entire understanding of the parties with respect to the subject matter hereof and supersedes all prior agreements, oral or written, and all other communications between the parties relating to such subject matter.

IN WITNESS WHEREOF, the parties hereto have executed this Business Associate Agreement as of the Effective Date.

BUSINESS ASSOCIATE

By

Date

Print Name

Title

COVERED ENTITY

By

Date

Print Name

Title