

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) is entered into as of the date listed in the Service Contract by and between the Covered Entity listed in the Memorandum of Agreement ("Covered Entity"), whose principal place of business is located at the address listed in the Memorandum of Agreement and the Vendor listed in the Memorandum of Agreement ("Business Associate"), whose principal place of business is located at the address listed in the Memorandum of Agreement, in conformance with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA RULES").

RECITALS

Whereas, the Covered Entity has engaged the services of the Business Associate for or on behalf of the Covered Entity in Memorandum of Agreement # _____;

Whereas, the Covered Entity must disclose individually identifiable health information to the Business Associate in the performance of the services for or on behalf of the Covered Entity;

Whereas, such information is Protected Health Information ("PHI") as defined under the HIPAA Rules;

Whereas, the Parties agree to establish safeguards for the protection of such information;

Whereas, the Covered Entity and Business Associate desire to enter into this Agreement to address certain requirements of the HIPAA Rules;

Therefore, the Parties agree as follows:

SECTION I – DEFINITIONS

Relevant terms in this Agreement shall have the same meaning as those terms in 45 CFR § 164.402; 45 CFR § 164.501; 45 CFR § 164.304; 45 CFR § 160.103, and the HIPAA Rules. The following terms, as defined in the HIPAA Rules, shall mean:

- 1.1 "Breach" is defined as any unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the PHI, unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based upon a risk assessment as required under 45 CFR § 164.402. Breach excludes:
 - a. Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business Associate, if performed in good faith and within the scope of authority, and does not result in further unauthorized disclosures;
 - b. Inadvertent one-time disclosure between Covered Entity or Business Associate workforce member to another workforce member at the same covered entity or Business Associate who is authorized to access PHI and information received or disclosed is not further used or disclosed in a manner not permitted under 45 CFR § 164.500 Subpart E; and
 - c. A disclosure where the Covered Entity or Business Associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.
- 1.2 "Business Associate" shall have the same meaning as under the HIPAA Rules, including, but not limited to, 45 CFR § 160.103.
- 1.3 "Covered Entity" shall have the same meaning as under the HIPAA Rules, including, but not limited to, 45 CFR § 160.103.
- 1.4 "Data Aggregation" shall have the same meaning as under the HIPAA Rules, including but not limited to, 45 CFR § 164.501.
- 1.5 "Designated Record Set" shall have the same meaning as under the HIPAA Rules, including, but not limited to 45 CFR § 164.501.
- 1.6 "Effective Date" shall be the Effective Date of this Agreement.

- 1.7 "Electronic Protected Health Information" or "Electronic PHI" shall have the same meaning as in 45 CFR § 160.103, limited to information of the Covered Entity that the Business Associate creates, receives, maintains, or transmits in electronic media on behalf of the Covered Entity under this Agreement.
- 1.8 "Health Care Operations" shall have the same meaning as under the HIPAA Rules, including, but not limited to, 45 CFR § 164.501.
- 1.9 "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules codified at 45 CFR Part 160 and 164, as may be amended from time to time.
- 1.10 "Individual" shall have the same meaning as in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative under 45 CFR § 164.502(g).
- 1.11 "Individually Identifiable Health Information" shall have the same meaning as under the HIPAA Rules, including, but not limited to 45 CFR § 160.103.
- 1.12 "Protected Health Information" or "PHI" shall have the same meaning as in the HIPAA Rules in 45 CFR § 160.103, limited to the information created, received, maintained, or transmitted by Business Associate from or on behalf of the Covered Entity.
- 1.13 "Required by Law" shall have the same meaning as in 45 CFR § 164.103.
- 1.14 "Secretary" shall mean the Secretary of the Department of Health and Human Services ("HHS") or his or her designee.
- 1.15 "Security Incident" shall have the same meaning as in 45 CFR § 164.304.
- 1.16 "Unsecured Protected Health Information" shall have the same meaning as in 45 CFR § 164.402 and shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary.

SECTION II – BUSINESS ASSOCIATE'S OBLIGATIONS AND ACTIVITIES

The Business Associate agrees to the following:

- 2.1 To fulfill its responsibilities under the contract setting out the scope of work for the Business Associate; To only use or further disclose PHI as permitted or required by this Agreement, by law, or for the proper management and administration of the Business Associate under Section III;
- 2.2 To use appropriate safeguards to comply with Subpart C of 45 CFR Part 164 with respect to Electronic PHI, to prevent the use or disclosure of PHI other than as provided for by this Agreement or as required by law;
- 2.3 To mitigate, to the extent practicable, any harmful known effect of a use or disclosure of PHI by the Business Associate in violation of this Agreement or the HIPAA Rules;
- 2.4 To immediately report to the Covered Entity any PHI use or disclosure not permitted by this Agreement of which it becomes aware, and in no event later than five (5) calendar days after discovery, including breaches of unsecured PHI as required by 45 CFR § 164.410, and any Security Incident of which it becomes aware under 45 CFR § 164.314, except as provided by 45 CFR § 164.412. In addition, the Business Associate shall provide the Covered Entity the following information: (1) a brief description of what happened, including the date of the breach and date of discovery of the breach, if known; (2) identification of each individual whose unsecured PHI has been affected by the breach; (3) a description of the type of unsecured PHI involved in the breach; (4) any steps the individuals should take to protect themselves from harm from the breach; (5) steps the Business Associate is taking to investigate the breach, mitigate harm, and protect against other breaches; and (6) and other information requested by the Covered Entity. The Business Associate, in consultation with the Covered Entity, shall be responsible for breach notifications to individuals affected by the unauthorized use or disclosure as required by 45 CFR § 164.404. The notifications shall be made no later than sixty (60) days following the discovery of the breach. A breach shall be treated as discovered as of the first day on which such breach is known to the Business Associate or, by exercising reasonable diligence, would have been known by the Business Associate. The Business Associate shall be solely responsible for all costs associated with the breach notifications. The Business Associate shall be responsible for any penalties, assessments, or fees assessed by the Office for Civil Rights/Department of HHS due to any breach caused by the Business Associate or based upon the failure of the Business Associate to comply

with the HIPAA Rules. The Business Associate, in consultation with the Covered Entity, shall make all required notices to the media and the Secretary on behalf of the Covered Entity.

- 2.5 In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any agent, including a subcontractor, that creates, receives, maintains, or transmits PHI on behalf of the Business Associate agrees in writing to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such PHI;
- 2.6 To the extent that the Business Associate maintains a Designated Record Set for the Covered Entity, to provide access to PHI in a Designated Record Set, at the request of the Covered Entity, and in the time and manner designated by the Covered Entity, to the Covered Entity, or as directed by the Covered Entity, to the Individual or the Individual's designee as necessary to meet the Covered Entity's obligations under 45 CFR § 164.524;
- 2.7 To the extent that the Business Associate maintains a Designated Record Set for the Covered Entity, to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of the Covered Entity or an Individual, and in the time and manner designated by the Covered Entity;
- 2.8 To make internal practices, books, and records, including policies and procedures on PHI, relating to the use and disclosure of PHI received from, created, or received by the Business Associate on behalf of the Covered Entity, available to the Covered Entity or the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for the Secretary to determine the Covered Entity's and the Business Associate's compliance with the HIPAA Rules;
- 2.9 To document non-routine disclosures of PHI and information related to such disclosures as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528, where applicable;
- 2.10 To provide the Covered Entity or an Individual, in a time and manner designated by the Covered Entity, information collected in accordance with Section 2.9 of this Agreement, to permit the Covered Entity to respond to a request for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528;
- 2.11 That if it creates, receives, maintains, or transmits any electronic PHI on behalf of the Covered Entity, it will implement administrative, physical, and technical safeguards in accordance with 45 CFR § 164.308, 45 CFR § 164.310, and 45 CFR § 164.312, and policies and procedures in accordance with 45 CFR § 164.316 that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI, and it will ensure that any agents (including subcontractors) it provides such Electronic PHI agree to implement reasonable and appropriate security measures to protect the information;
- 2.12 To retain records related to the PHI in accordance with 45 CFR 164.316 and 45 CFR 164.530 for a period of six (6) years beyond the date of the termination of this Agreement. In the event of termination of this Agreement, the provisions of Section VI shall govern record retention, return, or destruction;
- 2.13 To appropriately safeguard all PHI provided by the Covered Entity under the service contract or agreement as required under the HIPAA Rules and this Agreement, and to assure that any subcontractors provide satisfactory assurances as set out in 45 CFR § 164.502 (e) (1) and (2).
- 2.14 Not to make any fundraising communication on behalf of the Covered Entity or to the Covered Entity's participants and beneficiaries;
- 2.15 Not to receive any remuneration, either directly or indirectly, in exchange for PHI, except as may be permitted by 45 CFR § 164.502(a)(5) and 45 CFR § 164.508(a)(4);
- 2.16 Not to make any marketing communication on behalf of Covered Entity or to Covered Entity's participants and beneficiaries, except as may be permitted by 45 CFR § 164.501; and
- 2.17 To the extent the Business Associate is to carry out one or more of the Covered Entity's obligations 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 obligations.

SECTION III – THE PARTIES AGREE TO THE FOLLOWING

PERMITTED USES AND DISCLOSURES BY THE BUSINESS ASSOCIATE

- 3.1 Business Associate agrees to make uses, disclosures, and requests for PHI consistent with the Covered Entity's minimum necessary policies and procedures.
- 3.2 Except as otherwise limited in this Agreement, the Business Associate may use or disclose PHI to perform functions, activities, or services for or on behalf of the Covered Entity as specified in the Agreement, provided that such use or disclosure would not violate the HIPAA Rules if done by the Covered Entity; and
- 3.3 Except as otherwise limited in this Agreement, the Business Associate may:
 - a. Use PHI for the proper management and administration by the Business Associate or to carry out the legal responsibilities of the Business Associate; and
 - b. Disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that such disclosures are Required by Law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

SECTION IV – NOTICE OF PRIVACY PRACTICES

- 4.1 The Covered Entity shall (a) provide the Business Associate with the notice of privacy practices it produces in accordance with 45 CFR § 164.520, as well as any changes to such notice; (b) provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures; (c) notify the Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restrictions may affect the Business Associate's use or disclosure of PHI; and (d) refrain from requesting the Business Associate to use or disclose PHI in any impermissible manner under the HIPAA Rules if done by the Covered Entity.

SECTION V – BREACH NOTIFICATION REQUIREMENTS

- 5.1 The Business Associate shall notify each individual whose Unsecured PHI has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, used, or disclosed as a result of any Breach by the Business Associate:
 - a. Except as provided in 45 CFR § 164.412, the Business Associate shall provide notice without unreasonable delay and in no case later than sixty (60) days after discovery of a Breach or from the time it should have reasonably been discovered;
 - b. The notice shall be in plain language, including, to the extent possible:
 - 1) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
 - 2) A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - 3) Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
 - 4) A brief description of what the Business Associate is doing to investigate the Breach, mitigate harm to individuals, and protect against any further Breaches; and,
 - 5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.
 - c. In a method that meets the requirements of 45 CFR § 164.404(d); and

- d. The Business Associate shall provide for substitute notice, as required by the HIPAA Rules, by providing a toll-free phone number that remains active for at least ninety (90) days where an individual can learn whether the individual's unsecured PHI may have been included in the Breach and a posting as required by 45 CFR § 164.404 (d)(2). The Business Associate shall be responsible for the costs of the substitute notice and notifications.

SECTION VI – TERM AND TERMINATION

6.1 This Agreement shall be effective as of the date in the first paragraph and shall terminate when all of the PHI provided by the Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or if it is infeasible to return or destroy the PHI, protections are extended to such information as required in this Section.

6.2 Upon a material breach by either party, the non-breaching party shall provide an opportunity to cure the breach. The non-breaching party may terminate this Agreement and the Service Contract if the breach is not cured within the specified time. Either Party may immediately terminate this Agreement if it determines that a cure is not feasible.

If the Business Associate fails to cure a breach for which a cure is reasonably possible, the Covered Entity may take action to cure the breach, including but not limited to, obtaining an injunction that will prevent further improper use or disclosure of PHI. Should such action be taken, the Business Associate agrees to indemnify the Covered Entity for any costs, including court costs and attorneys' fees, associated with curing the breach.

6.3 Effect of Termination.

a. Return or Destruction of PHI. Except as provided in Section 6.3(b), upon termination of this Agreement, the Business Associate shall return or if agreed to by the Covered Entity, destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of PHI.

b. Return or Destruction of PHI Infeasible. If the Business Associate determines that returning or destroying PHI is infeasible, the Business Associate shall notify the Covered Entity of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that the return or destruction of the PHI is infeasible, the 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 the Business Associate maintains such PHI. In addition, the Business Associate shall continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 to prevent use or disclosure of the PHI for as long as the Business Associate retains the PHI.

SECTION VII – GENERAL PROVISIONS

7.1 Compliance with Law. In connection with its performance under this Agreement, Business Associate shall comply with all applicable laws.

7.2 Amendment. The Parties agree to amend this Agreement if necessary to comply with the HIPAA Rules and any other applicable law. This Agreement may not be modified, nor shall any provision be waived, except in a writing signed by the Parties. A waiver with respect to one event shall not be construed as continuing or as a bar to or waiver of any right or remedy as to subsequent events.

7.3 Confidentiality Obligations. In performing under this Agreement, each Party may receive, be exposed to, or acquire "Confidential Information," including but not limited to, information, data, reports, summaries, tables and studies, whether written or oral, fixed in hard copy or contained in a computer data base or computer readable form, of the other Party. For purposes of this Agreement, "Confidential Information" shall not apply to PHI, the privacy and security of which is the subject of this Agreement. The Parties, including their employees, agents and representatives shall: (a) not disclose to any third-party "Confidential Information" of the other party except as permitted under this Agreement; (b) only permit the use of "Confidential Information" of employees, agents, or representatives having a need to know under this Agreement, and (c) advise each of its employees, agents, and representatives of their obligations to keep such "Confidential Information" confidential. This provision shall not apply to "Confidential Information": (i) after it becomes publicly available through no fault of either Party; (ii) which is later publicly released, in writing, by the party that owned the material; (iii) which is lawfully obtained by third parties without restriction; or (iv) which can be shown to be previously known or developed by either party independently of the other party.

- 7.4 No Third-Party Beneficiary. The Parties do not express or imply by any terms in this Agreement to confer any rights, remedies, or entitlements upon any third person not a party to this Agreement.
- 7.5 Indemnification by Business Associate. Business Associate agrees to indemnify, defend and hold harmless the Covered Entity and its employees, directors, officers, subcontractors, agents or other members of its workforce, ("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 Business Associate's actions arising out of this Agreement. Accordingly, on demand, Business Associate shall reimburse any Indemnified Party for all actual and direct losses, liabilities, fines, penalties, costs or expenses (including reasonable attorneys' fees) that may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party that results from Business Associate's breach. The obligation to indemnify any Indemnified Party shall survive the expiration or termination of this Agreement.
- 7.6 Survival. The rights and obligations of the Business Associate under Section II and Section 6.3(b) of this Agreement shall survive the termination of this Agreement.
- 7.7 Interpretation. Any ambiguity in this Agreement shall be resolved to permit the Covered Entity to comply with the HIPAA Rules.
- 7.8 Notices. Notices to be given to a Party shall be made in writing via certified U.S. Mail to such Party's address listed in the Service Contract, and/or via facsimile to the facsimile telephone numbers listed in the Service Contract. If an email address is provided below, notice may be submitted via email, if agreed upon between the Parties.
- Each party named in the Service Contract may update its address and that of its representative for notice by giving notice thereof in the provided manner.
- 7.9 Counterparts: This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies shall be deemed to be originals.
- 7.10 Disputes. If any controversy, dispute, or claim arises between the Parties with respect to this Agreement, the Parties shall make good faith efforts to resolve such matters informally. Any dispute that cannot be mutually settled may be brought in the Franklin Circuit Court or Federal District Court of Kentucky.
- 7.11 Mutual Representations and Warranties. Each Party represents and warrants that it is duly organized, validly existing, and in good standing under the laws of the jurisdiction under which it is organized or licensed; it has the full power to enter into this Agreement and to perform its obligations; and that the performance of its obligations under this Agreement have been duly authorized and will not violate any provisions of any license, corporate charter, or bylaws.

Wherefore, the Parties acknowledge agreement with the above terms and execute this Agreement as of the Effective Date by their signatures below.

Covered Entity

Business Associate

By:

By

Name:

Name:

Title:

Title:

Date:

Date: