

ATTACHMENT 1
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) REQUIREMENTS

- 1.1 Health Insurance Portability and Accountability Act of 1996, as amended - The Owner and the Contractor are both subject to and must comply with provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) (PL-111-5) (collectively, and hereinafter, HIPAA) and all regulations promulgated pursuant to authority granted therein. The Contractor constitutes a “Business Associate” of the Owner as such term is defined in the Code of Federal Regulations (CFR) at 45 CFR 160.103. Therefore, the term, “Contractor” as used in this section shall mean “Business Associate.”
- a. The Contractor shall agree and understand that for purposes of the Business Associate Provisions contained herein, terms used but not otherwise defined shall have the same meaning as those terms defined in 45 CFR parts 160 and 164 and 42 U.S.C. §§ 17921 *et. seq.* including, but not limited to the following:
- 1) “Access”, “administrative safeguards”, “confidentiality”, “covered entity”, “data aggregation”, “designated record set”, “disclosure”, “hybrid entity”, “information system”, “physical safeguards”, “required by law”, “technical safeguards”, “use” and “workforce” shall have the same meanings as defined in 45 CFR 160.103, 164.103, 164.304, and 164.501 and HIPAA.
 - 2) “Breach” shall mean the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such information, except as provided in 42 U.S.C. § 17921. This definition shall not apply to the term “breach of contract” as used within the contract.
 - 3) “Electronic Protected Health Information” shall mean information that comes within paragraphs (1)(i) or (1)(ii) of the definition of Protected Health Information as specified below.
 - 4) “Enforcement Rule” shall mean the HIPAA Administrative Simplification: Enforcement; Final Rule at 45 CFR parts 160 and 164.
 - 5) “Individual” shall have the same meaning as the term “individual” in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502 (g).
 - 6) “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.
 - 7) “Protected Health Information” as defined in 45 CFR 160.103, shall mean individually identifiable health information:
 - (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; or (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
 - (2) Protected Health Information excludes individually identifiable health information in (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity (Owner) in its role as employer.
 - 8) “Security Incident” shall be defined as set forth in the “Obligations of the Contractor” section of the Business Associate Provisions.
 - 9) “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR part 164, subpart C.
 - 10) “Unsecured Protected Health Information” shall mean Protected Health Information that is not secured through the use of a technology or methodology determined in accordance with 42 U.S.C. § 17932 or as otherwise specified by the secretary of Health and Human Services.
- b. The Contractor agrees and understands that wherever in this document the term Protected Health Information is used, it shall also be deemed to include Electronic Protected Health Information.

- c. The Contractor must appropriately safeguard Protected Health Information which the Contractor receives from or creates or receives on behalf of the Owner. To provide reasonable assurance of appropriate safeguards, the Contractor shall comply with the Business Associate Provisions stated herein.
- d. The Owner and the Contractor agree to amend the contract as is necessary for the parties to comply with the requirements of HIPAA and the Privacy Rule, Security Rule, Enforcement Rule, and other rules as later promulgated (hereinafter referenced as the regulations promulgated thereunder).

1.2 Permitted uses and disclosures of Protected Health Information:

- a. The Contractor may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, the Owner as specified in the contract, provided that such use or disclosure would not violate HIPAA and the regulations promulgated thereunder.
- b. The Contractor may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1) and shall notify the Owner by no later than ten (10) calendar days after the Contractor becomes aware of the disclosure of the Protected Health Information.
- c. If required to properly perform the contract and subject to the terms of the contract, the Contractor may use or disclose Protected Health Information if necessary for the proper management and administration of the Contractor's business.
- d. If the disclosure is required by law, the Contractor may disclose Protected Health Information to carry out the legal responsibilities of the Contractor.
- e. The Contractor may use Protected Health Information to provide Data Aggregation services to the Owner as permitted by 45 CFR 164.504(e)(2)(i)(B).

1.3 Obligations of the Contractor:

- a. The Contractor shall not use or disclose Protected Health Information other than as permitted or required by the contract or as otherwise required by law, and shall comply with the minimum necessary disclosure requirements set forth in 45 CFR § 164.502(b).
- b. The Contractor shall use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by the contract. Such safeguards shall include, but not be limited to:
 - 1) Workforce training on the appropriate uses and disclosures of Protected Health Information pursuant to the terms of the contract.
 - 2) Policies and procedures implemented by the Contractor to prevent inappropriate uses and disclosures of Protected Health Information by its workforce.
 - 3) Encryption of any portable device used to access or maintain protected health information or use of equivalent safeguard.
 - 4) Encryption of any transmission of electronic communication containing protected health information or use of equivalent safeguard.
 - 5) Any other safeguards necessary to prevent the inappropriate use or disclosure of Protected Health Information.
- c. With respect to Electronic Protected Health Information, the Contractor shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic Protected Health Information that Contractor creates, receives, maintains or transmits on behalf of the Owner.

- d. The Contractor shall require that any agent or subcontractor to whom the Contractor provides any Protected Health Information received from, created by, or received by the Contractor pursuant to the contract, also agrees to the same restrictions and conditions stated herein that apply to the Contractor with respect to such information.
- e. By no later than ten (10) calendar days of receipt of a written request from the Owner, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the Owner, the Contractor shall make the Contractor's internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, created by, or received by the Contractor on behalf of the Owner available to the Owner and/or to the Secretary of the Department of Health and Human Services or designee for purposes of determining compliance with the Privacy Rule.
- f. The Contractor shall document any disclosures and information related to such disclosures of Protected Health Information as would be required for the Owner to respond to a request by an individual for an accounting of disclosures of Protected Health Information in accordance with 42 USCA §17932 and 45 CFR 164.528. By no later than five (5) calendar days of receipt of a written request from the Owner, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the Owner, the Contractor shall provide an accounting of disclosures of Protected Health Information regarding an individual to the Owner. If requested by the Owner or the individual, the Contractor shall provide an accounting of disclosures directly to the individual. The Contractor shall maintain a record of any accounting made directly to an individual at the individual's request and shall provide such record to the Owner upon request.
- g. In order to meet the requirements under 45 CFR 164.524, regarding an individual's right of access, the Contractor shall, within five (5) calendar days following a Owner request, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the Owner, provide the Owner access to the Protected Health Information in an individual's designated record set. However, if requested by the Owner, the Contractor shall provide access to the Protected Health Information in a designated record set directly to the individual for whom such information relates.
- h. At the direction of the Owner, the Contractor shall promptly make any amendment(s) to Protected Health Information in a Designated Record Set pursuant to 45 CFR 164.526.
- i. The Contractor shall report to the Owner's Security Officer any security incident immediately upon becoming aware of such incident and shall take immediate action to stop the continuation of any such incident. For purposes of this paragraph, security incident shall mean the attempted or successful unauthorized access, use, modification or destruction of information or interference with systems operations in an information system. This does not include trivial incidents that occur on a daily basis, such as scans, "pings," or unsuccessful attempts that do not penetrate computer networks or servers or result in interference with system operations. By no later than five (5) days after the Contractor becomes aware of such incident, the Contractor shall provide the Owner's Security Officer with a description of any remedial action taken to mitigate any harmful effect of such incident and a proposed written plan of action for approval that describes plans for preventing any such future security incidents.
- j. The Contractor shall report to the Owner's Privacy Officer any unauthorized use or disclosure of Protected Health Information not permitted or required as stated herein immediately upon becoming aware of such use or disclosure and shall take immediate action to stop the unauthorized use or disclosure. By no later than five (5) calendar days after the Contractor becomes aware of any such use or disclosure, the Contractor shall provide the Owner's Privacy Officer with a written description of any remedial action taken to mitigate any harmful effect of such disclosure and a proposed written plan of action for approval that describes plans for preventing any such future unauthorized uses or disclosures.

- k. The Contractor shall report to the Owner's Security Officer any breach immediately upon becoming aware of such incident and shall take immediate action to stop the continuation of any such incident. By no later than five (5) days after the Contractor becomes aware of such incident, the Contractor shall provide the Owner's Security Officer with a description of any remedial action taken to mitigate any harmful effect of such incident and a proposed written plan for approval that describes plans for preventing any such future incidents.
- l. The Contractor's reports specified in the preceding paragraphs shall include the following information regarding the security incident, improper disclosure/use, or breach, (hereinafter "incident"):
 - 1) The name, address, and telephone number of each individual whose information was involved if such information is maintained by the Contractor;
 - 2) The electronic address of any individual who has specified a preference of contact by electronic mail;
 - 3) A brief description of what happened, including the date(s) of the incident and the date(s) of the discovery of the incident;
 - 4) A description of the types of Protected Health Information involved in the incident (such as full name, Social Security Number, date of birth, home address, account number, or disability code) and whether the incident involved Unsecured Protected Health Information; and
 - 5) The recommended steps individuals should take to protect themselves from potential harm resulting from the incident.
- m. Notwithstanding any provisions of the Terms and Conditions attached hereto, in order to meet the requirements under HIPAA and the regulations promulgated thereunder, the Contractor shall keep and retain adequate, accurate, and complete records of the documentation required under these provisions for a minimum of six (6) years as specified in 45 CFR part 164.
- n. Contractor shall not directly or indirectly receive remuneration in exchange for any protected health information without a valid authorization.
- o. If the Contractor becomes aware of a pattern of activity or practice of the Owner that constitutes a material breach of contract regarding the Owner's obligations under the Business Associate Provisions of the contract, the Contractor shall notify the Owner's Security Officer of the activity or practice and work with the Owner to correct the breach of contract.
- p. The Contractor shall indemnify the Owner from any liability resulting from any violation of the Privacy Rule or Security Rule or Breach arising from the conduct or omission of the Contractor or its employee(s), agent(s) or subcontractor(s). The Contractor shall reimburse the Owner for any and all actual and direct costs and/or losses, including those incurred under the civil penalties implemented by legal requirements, including but not limited to HIPAA as amended by the Health Information Technology for Economic and Clinical Health Act, and including reasonable attorney's fees, which may be imposed upon the Owner under legal requirements, including but not limited to HIPAA's Administrative Simplification Rules, arising from or in connection with the Contractor's negligent or wrongful actions or inactions or violations of this Agreement.

1.4 Obligations of the Owner:

- a. The Owner shall notify the Contractor of limitation(s) that may affect the Contractor's use or disclosure of Protected Health Information, by providing the Contractor with the Owner's notice of privacy practices in accordance with 45 CFR 164.520.
- b. The Owner shall notify the Contractor of any changes in, or revocation of, authorization by an Individual to use or disclose Protected Health Information.

- c. The Owner shall notify the Contractor of any restriction to the use or disclosure of Protected Health Information that the Owner has agreed to in accordance with 45 CFR 164.522.
 - d. The Owner shall not request the Contractor to use or disclose Protected Health Information in any manner that would not be permissible under HIPAA and the regulations promulgated thereunder.
- 1.5 Expiration/Termination/Cancellation - Except as provided in the subparagraph below, upon the expiration, termination, or cancellation of the contract for any reason, the Contractor shall, at the discretion of the Owner, either return to the Owner or destroy all Protected Health Information received by the Contractor from the Owner, or created or received by the Contractor on behalf of the Owner, and shall not retain any copies of such Protected Health Information. This provision shall also apply to Protected Health Information that is in the possession of subcontractor or agents of the Contractor.
- a. In the event the Owner determines that returning or destroying the Protected Health Information is not feasible, the Contractor shall extend the protections of the contract to the Protected health Information for as long as the Contractor maintains the Protected Health Information and shall limit the use and disclosure of the Protected Health Information to those purposes that made return or destruction of the information infeasible. If at any time it becomes feasible to return or destroy any such Protected Health Information maintained pursuant to this paragraph, the Contractor must notify the Owner and obtain instructions from the Owner for either the return or destruction of the Protected Health Information.
- 1.6 Breach of Contract – In the event the Contractor is in breach of contract with regard to the Business Associate Provisions included herein, the Contractor shall agree and understand that in addition to the requirements of the contract related to cancellation of contract, if the Owner determines that cancellation of the contract is not feasible, the State of Missouri may elect not to cancel the contract, but the Owner shall report the breach of contract to the Secretary of the Department of Health and Human Services.