

## 1.1 Business Associate Provisions:

Make sure the “state agency” is adequately defined previously in the contract/bid document. If not, then be sure to indicate the specific section of the “state agency” that is subject to HIPAA. If you refer to the contractor by another name, (e.g.: provider, vendor, etc), be sure to change all references to the contractor in the following provisions.

1.1.1 Health Insurance Portability and Accountability Act of 1996, as amended - The state agency 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 state agency. Therefore, the term, “contractor” as used in this section shall mean “Business Associate.”

a. The contractor agrees 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) “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the contractor.
- 4) “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the state agency.
- 5) “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.
- 6) “Enforcement Rule” shall mean the HIPAA Administrative Simplification: Enforcement; Final Rule at 45 CFR Parts 160 and 164.
- 7) “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- 8) “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).
- 9) “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.
- 10) “Protected Health Information” as defined in 45 CFR 160.103, shall mean individually identifiable health information:
  - (a) Except as provided in paragraph (b) 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.

- (b) 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 (state agency) in its role as employer.

11) "Security Incident" shall be defined as set forth in the "Obligations of the Contractor" section of the Business Associate Provisions.

12) "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 164, Subpart C.

13) "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 state agency. To provide reasonable assurance of appropriate safeguards, the contractor shall comply with the business associate provisions stated herein, as well as the 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) and all regulations promulgated pursuant to authority granted therein.

d. The state agency 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). Any ambiguity in the contract shall be interpreted to permit compliance with the HIPAA Rules.

#### 1.1.2 Permitted Uses and Disclosures of Protected Health Information by the Contractor:

a. The contractor may not use or disclose Protected Health Information in any manner that would violate Subpart E of 45 CFR Part 164 if done by the state agency, except for the specific uses and disclosures in the contract.

b. The contractor may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, the state agency as specified in the contract, provided that such use or disclosure would not violate HIPAA and the regulations promulgated thereunder.

c. 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 state agency by no later than ten (10) calendar days after the contractor becomes aware of the disclosure of the Protected Health Information.

d. 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.

e. If the disclosure is required by law, the contractor may disclose Protected Health Information to carry out the legal responsibilities of the contractor.

f. If applicable, the contractor may use Protected Health Information to provide Data Aggregation services to the state agency as permitted by 45 CFR 164.504(e)(2)(i)(B).

- g. The contractor may not use Protected Health Information to de-identify or re-identify the information in accordance with 45 CFR 164.514(a)-(c) without specific written permission from the state agency to do so.
- h. The contractor agrees to make uses and disclosures and requests for Protected Health Information consistent with the state agency's minimum necessary policies and procedures.

### 1.1.3 Obligations and Activities 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 and subcontractors, if applicable;
  - 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; and
  - 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 use appropriate 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 state agency and comply with Subpart C of 45 CFR Part 164, to prevent use or disclosure of Protected Health Information other than as provided for by the contract.
- d. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), the contractor shall require that any agent or subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of the contractor agrees to the same restrictions, conditions, and requirements that apply to the contractor with respect to such information.
- e. By no later than ten (10) calendar days after receipt of a written request from the state agency, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the state agency, 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 state agency available to the state agency and/or to the Secretary of the Department of Health and Human Services or designee for purposes of determining compliance with the HIPAA Rules and the contract.
- f. The contractor shall document any disclosures and information related to such disclosures of Protected Health Information as would be required for the state agency 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 state agency, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the state agency, the contractor shall provide an accounting of disclosures of Protected Health Information regarding an individual to the state agency. If requested by the state agency 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 state agency 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 state agency 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 state agency, provide the state agency access to the Protected Health Information in an individual's designated record set. However, if requested by the state agency, 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 state agency, 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 state agency'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 state agency'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 state agency'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 state agency'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 state agency'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 state agency's Security Officer with a description of the breach, the information compromised by the breach, and 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 required 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 state agency that constitutes a material breach of contract regarding the state agency's obligations under the Business Associate Provisions of the contract, the contractor shall notify the state agency's Security Officer of the activity or practice and work with the state agency to correct the breach of contract.
  - p. The contractor shall indemnify the state agency 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 state agency 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 state agency 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.

#### 1.1.4 Obligations of the State Agency:

- a. The state agency 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 state agency's notice of privacy practices in accordance with 45 CFR 164.520.
- b. The state agency shall notify the contractor of any changes in, or revocation of, authorization by an Individual to use or disclose Protected Health Information.
- c. The state agency shall notify the contractor of any restriction to the use or disclosure of Protected Health Information that the state agency has agreed to in accordance with 45 CFR 164.522.
- d. The state agency 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.

1.1.5 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 state agency, either return to the state agency or destroy all Protected Health Information received by the contractor from the state agency, or created or received by the contractor on behalf of the state agency, 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 state agency 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 state agency and obtain instructions from the state agency for either the return or destruction of the Protected Health Information.

1.1.6 Breach of Contract – In the event the contractor is in breach of contract with regard to the business associate provisions included herein, the contractor agrees that in addition to the requirements of the contract related to cancellation of contract, if the state agency determines that cancellation of the contract is not feasible, the State of Missouri may elect not to cancel the contract, but the state agency shall report the breach of contract to the Secretary of the Department of Health and Human Services.

#### **END OF BUSINESS ASSOCIATE PROVISIONS**

Make sure the contract includes cancellation/breach of contract provisions such as the standard provisions included in the Division of Purchasing and Materials Management's (DPMM) Terms and Conditions:

#### **16. CANCELLATION OF CONTRACT**

- a. In the event of material breach of the contractual obligations by the contractor, the DPMM may cancel the contract. At its sole discretion, the DPMM may give the contractor an opportunity to cure the breach or to explain how the breach will be cured. The actual cure must be completed within no more than 10 working days from notification, or at a minimum the contractor must provide DPMM within 10 working days from notification a written plan detailing how the contractor intends to cure the breach.
- b. If the contractor fails to cure the breach or if circumstances demand immediate action, the DPMM will issue a notice of cancellation terminating the contract immediately. If it is determined the DPMM improperly cancelled the contract, such cancellation shall be deemed a termination for convenience in accordance with the contract.
- c. If the DPMM cancels the contract for breach, the DPMM reserves the right to obtain the equipment, supplies, and/or services to be provided pursuant to the contract from other sources and upon such terms and in such manner as the DPMM deems appropriate and charge the contractor for any additional costs incurred thereby.
- d. The contractor understands and agrees that funds required to fund the contract must be appropriated by the General Assembly of the State of Missouri for each fiscal year included within the contract period. The contract shall not be binding upon the state for any period in which funds have not been appropriated, and the state shall not be liable for any costs associated with termination caused by lack of appropriations.

Revised 5/15/13