BUSINESS ASSOCIATE ADDENDUM (PRIVACY AND SECURITY)

I. BUSINESS ASSOCIATE AGREEMENT

Section 1. **Use of Protected Health Information**. Contractor (hereinafter "Business Associate") may use PHI to provide the services under the Agreement. Business Associate shall not use PHI received from HHSC in any manner that would constitute a violation of the Privacy Rule if so used by HHSC or a violation of this Exhibit. Business Associate shall further ensure that its directors, officers, employees, contractors, and agents do not use PHI received from HHSC in any manner that would constitute a violation of the Privacy Rule if so used by HHSC or a violation of this Exhibit. Business Associate may use PHI for Business Associate's proper management and administrative services, or to carry out the legal responsibilities of Business Associate. Business Associate will not use PHI to create de-identified information for purposes unrelated to providing the services under the Agreement without HHSC's advance approval. Business Associate will use and request only the minimum PHI necessary to accomplish the permissible purpose of the use or request and will comply with HHSC's minimum necessary policies.

Section 2. **Business Associate's Acknowledgement.** Business Associate acknowledges its obligation to, and shall, comply with the HIPAA Security Rule, the Breach Notification Rule, and certain provisions of the HIPAA Privacy Rule and hereby agrees to comply with same.

Section 3. **Disclosure of PHI**. Business Associate may disclose PHI to provide the services under the Agreement. Business Associate shall not disclose PHI received from HHSC in any manner that would constitute a violation of the Privacy Rule if so disclosed by HHSC or a violation of this Exhibit. Business Associate shall further ensure that its directors, officers, employees, contractors, and agents do not disclose PHI received from HHSC in any manner that would constitute a violation of the Privacy Rule if so disclosed by HHSC or a violation of this Exhibit. Business Associate may disclose PHI only in a manner permitted pursuant to this Exhibit or as required by law. Business Associate will disclose and request only the minimum PHI necessary to accomplish the permissible purpose of the disclosure or request, and will comply with HHSC's minimum necessary policies.

If Business Associate discloses PHI to a third party, Business Associate must obtain, prior to making any such disclosure: (1) reasonable assurances from such third party that such PHI will be held confidential as provided pursuant to this Addendum, and only disclosed as required by law or for the purposes for which it was disclosed to such third party; (2) an agreement from such third party to immediately notify Business Associate of any breaches of the confidentiality of the PHI, to the extent it has obtained knowledge of such breach.

Section 4. **Safeguards Against Misuse of Information**. Business Associate agrees that it will implement all appropriate safeguards to prevent the use or disclosure of PHI other than pursuant to the terms and conditions of this Addendum.

Section 5. **Safeguards to Protect the Confidentiality, Integrity, and Availability of Electronic PHI**. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains, or transmits on behalf of HHSC as required by the Security Rule. Business Associate shall further ensure that its directors, officers, employees, contractors, subcontractors, and any other agents to whom it provides such information agree to implement reasonable and appropriate safeguards to protect it.

Section 6. **Reporting of Disclosures and Uses of PHI**. Business Associate shall, within **three (3) business days** of becoming aware of a disclosure or use of PHI in violation of this Exhibit, including a breach of unsecured PHI as provided in the Breach Notification Rule, by Business Associate, its officers, directors, employees, contractors, or agents, or by a third party to which Business Associate disclosed PHI pursuant to Section 3 of this Exhibit, report any such disclosure or use to HHSC. Business Associate shall mitigate to the extent practicable any harmful effect that is known or is likely resulting from a use or disclosure in violation of this Exhibit and/or of HIPAA.

Section 7. **Reporting of Security Incidents**. Pursuant to the Security Rule, Business Associate shall, within **three (3) business days** of becoming aware of any security incident, including a breach of unsecured PHI, report such security incident to HHSC.

Section 8. **Costs of Notification.** Business Associate is responsible for any and all costs incurred for notification of individuals or their representatives, as required by applicable authority including but not limited to 45 CFR 164.400 et seq, and for mitigation of any known or likely harm (including but not limited to reasonable costs for credit monitoring and credit restoration services for affected individuals) resulting from any privacy breach or security incident committed by Business Associate, its officers, directors, employees, contractors or agents, or by a third party to which Business Associate disclosed PHI pursuant to Section 3 of this Agreement. This provision shall survive termination of the Agreement.

Section 9. **Agreements by Third Parties**. Business Associate shall not allow any third party to create, receive, maintain, or transmit PHI on Business Associate's behalf unless: (a) required by law; or (b) as permitted by this Exhibit and the Agreement. Business Associate shall ensure that any subcontractor that creates, receives, maintains, or transmits PHI on Business Associate's behalf agrees in writing to: (i) the same or more stringent restrictions, terms, and conditions that apply through this Exhibit to Business Associate with respect to such PHI; and (ii) comply with the applicable provisions of the Security Rule. Vendor shall not disclose PHI to any person outside of the United States without the written approval of HHSC. Business Associate shall not allow a subcontractor to create, receive, maintain, or transmit PHI on Business Associate's behalf unless Business Associate first has conducted reasonable due diligence of the subcontractor's information security and determined that such security is reasonable.

Section 10. **Access to Information**. Within five (5) days of a request by HHSC for access to PHI about an individual contained in a Designated Record Set, Business Associate shall make available to HHSC such PHI, for so long as such information is maintained in the Designated Record Set. In the event any individual requests access to PHI directly from Business Associate, Business Associate shall within two (2) days forward such request to HHSC. Any decision to deny access to PHI requested by an individual shall be made only by HHSC.

Section 11. **Availability of PHI for Amendment**. Within five (5) days of receipt of a request from HHSC for the amendment of an individual's PHI or record regarding an individual (for so long as the PHI is maintained), Business Associate shall provide such information to HHSC for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526, as amended from time to time.

Section 12. **Accounting of Disclosures**. Within ten (10) days of notice by HHSC to Business Associate that HHSC has received a request for an accounting of disclosures of PHI regarding an individual made during a period of time less than six (6) years prior to the date on which the accounting was requested, Business Associate shall make available to HHSC such information as is in Business Associate's possession and is required for HHSC to make the accounting required by 45 C.F.R. §164.528, as amended from time to time. At a minimum, Business Associate shall provide HHSC with the following information: (1) the date of the disclosure; (2) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (3) a brief description of the PHI disclosed; and (4) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall within two (2) days forward such request to HHSC. It shall be the responsibility of HHSC to prepare and deliver any such accounting requested. Business Associate hereby agrees to implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section.

Section 13. **Availability of Books and Records**. Business Associate hereby agrees to make 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, HHSC available to the Secretary for purposes of determining HHSC's and Business Associate's compliance with HIPAA and to HHSC for purposes of determining Business Associate's compliance with this Exhibit and HIPAA. Business Associate shall: (a) immediately notify HHSC of any request from the Secretary under this Section; (b) cooperate with HHSC in furnishing requested materials; and (c) provide a copy to HHSC of any materials furnished to the Secretary under this Section. Nothing in this Section shall be construed as waiving any privilege or discovery protection, including with respect to trade secrets and confidential commercial information.

Section 14. **Covered Entity Obligations**. To the extent that Business Associate is to carry out one or more of HHSC's covered obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to HHSC in the performance of such obligations.

Section 15. **No Sale of PHI**. Business Associate shall not directly or indirectly pay or receive remuneration in exchange for PHI or otherwise engage in the sale of PHI in a manner that would be impermissible for Business Associate under HIPAA or would be impermissible if done by HHSC under HIPAA. Business Associate shall not act in a manner that would cause HHSC to not be in compliance with such prohibition.

Section 16. **Sanctions**. Business Associate shall impose appropriate sanctions on any workforce member who fails to act in accordance with this Exhibit and/or HIPAA.

Section 17. **Compliance with Applicable Law**. Business Associate shall comply with applicable federal and state confidentiality, privacy, and security laws, including, but not limited to, HIPAA. Business Associate shall not act or fail to act in a manner that would cause, directly or indirectly, HHSC to not be in compliance with applicable federal or state law.

Section 18. **Commencement and Termination of Electronic Access by Business Associate's Employees and Subcontractors**. Within ten (10) days of signature of this Agreement, Business Associate shall provide HHSC with a list of individual employees and subcontractors who will require access to HHSC's electronic and computer systems in order to perform duties pursuant to Business Associate's agreement with HHSC. Business Associate shall require all such persons to execute additional confidentiality documentation prior to receiving such access. If any such person terminates employment or contract status with Business Associate or its subcontractors, Business Associate shall notify HHSC no later than **five (5) business days** in advance of same, or in any event immediately upon termination, so that HHSC may terminate the individual's access to HHSC's systems.

Section 19. **Return and Destruction of PHI**. At termination of the Agreement, Business Associate shall either return or destroy all PHI received from, or created or received by Business Associate on behalf of, HHSC that Business Associate still maintains in any form. Business Associate shall further not retain any copies of such information in any form. In the event such return or destruction is not feasible, Business Associate shall (1) provide an explanation in writing to HHSC as to why such return or destruction is not feasible to HHSC's satisfaction; (2) continue to extend the protection required under this Addendum; and (3) limit any further uses and disclosures of the PHI to those purposes that make the return or destruction of the information infeasible. This provision shall survive the termination of this Agreement.

Section 20. **Termination for Violation**. Notwithstanding any other provisions of the Agreement to the contrary, if HHSC determines that Business Associate has materially breached or violated its obligations under this Addendum, and reasonable efforts to cure the breach or to end the violation are unsuccessful, HHSC shall have the right, but not the duty, to terminate this Agreement.

II. DEFINITIONS FOR USE IN THIS ADDENDUM

Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy Rule, Breach Notification Rule, or the Security Rule.

“Breach Notification Rule” shall mean the Breach Notification of Unsecured Protected Health Information Rule, 45 CFR Part 164, Subparts A and D.

"Designated Record Set" shall mean a group of records maintained by or for HHSC that is (1) the medical records and billing records about individuals maintained by or for HHSC, (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for HHSC to make decisions about individuals. As used herein, the term “Record” means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for HHSC.

"Electronic Media" shall mean the mode of electronic transmissions. It includes the Internet, extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

"Individually Identifiable Health Information" shall mean information that is a subset of health information, including demographic information collected from an individual, and:

(1) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

(2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and

  (a) that identifies the individual, or

  (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Privacy Rule" shall mean the Standard for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and E, as amended from time to time.

"Protected Health Information" (or "PHI") shall mean Individually Identifiable Health Information that is (1) transmitted by electronic media; (2) maintained in any medium constituting electronic media; or (3) transmitted or maintained in any other form or medium. "PHI" shall not include: education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. §1232g; records described in 20 U.S.C. §1232g (a)(4)(B)(iv); employer records; or information about an individual who has been deceased for more than 50 years.

"Secretary" shall mean the Secretary of the United States Department of Health and Human Services.

"Security Incident" shall mean any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

"Security Rule" shall mean the Security Standard for electronic Protected Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and C, as amended from time to time.

[The remainder of this page is intentionally left blank.]