

PRIVACY AND SECURITY ADDENDUM

1. BUSINESS ASSOCIATE AGREEMENT

Section 1. Use of Protected Health Information. Contractor shall not use Protected Health Information (hereinafter "PHI") received from HHSC in any manner that would constitute a violation of the Privacy Standards if so used by HHSC. Contractor 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 Standards if so used by HHSC. Contractor may use PHI for Contractor's proper management and administrative services, or to carry out the legal responsibilities of the Contractor.

Section 2. Contractor's Acknowledgment. Contractor acknowledges its obligation to comply with the HIPAA Security Rule (45 CFR Sections 164.302 through 164.318) and the use and disclosure provisions of the HIP AA Privacy Rule (45 CFR Sections 164.502 and 164.504), and hereby agrees to comply with same.

Section 3. Disclosure of PHI. Contractor shall not disclose PHI received from HHSC in any manner that would constitute a violation of the Privacy Standards if so disclosed by HHSC. Contractor 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 Standards if so used by HHSC. Contractor may disclose PHI in a manner permitted pursuant to this Privacy Addendum (hereinafter "Addendum") or as required by law. If Contractor discloses PHI to a third party, Contractor 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; and (2) an agreement from such third party to immediately notify Contractor 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. Contractor 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. Contractor 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 Standards. Contractor shall further ensure that its directors, officers, employees, contractors, subcontractors, and any other agent to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it.

employees, contractors, or agents, or by a third party to which Contractor disclosed PHI pursuant to Section 2 of this Addendum, report any such Privacy Breach to HHS C by providing notification in the method and format required by 45 CFR 164.410.

Section 7. Reporting of Security Incidents. Pursuant to the Security Standards, Contractor shall, within three (3) business days of becoming aware of any security incident, report such security incident to HHSC.

Section 8. Costs of Notification. Contractor 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, resulting from any Privacy Breach or security incident committed by Contractor, its officers, directors, employees, contractors or agents, or by a third party to which Contractor disclosed PHI pursuant to Section 2 of this Addendum.

Section 9. Agreements by Third Parties. If an agent, including a subcontractor, will have access to PHI that is received from, or created by the Contractor on behalf of, HHSC, Contractor shall enter into an agreement with such an agent, pursuant to which agreement the agent agrees to be bound by the same restrictions, terms, and conditions that apply to Contractor pursuant to this Addendum with respect to such PHI.

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, Contractor 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 Contractor, Contractor 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 ten (10) days of receipt of a request from HHSC for the amendment of an individual's PHI or record regarding an individual contained in a Designated Record Set (for so long as the PHI is maintained in the Designated Record Set), Contractor 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 Contractor 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, Contractor shall make available to HHSC such information as is in Contractor'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, Contractor 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

accounting requested. Contractor 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. Contractor 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 Contractor on behalf of, HHSC available to the Secretary for purposes of determining HHSC's and Contractor's compliance with the Privacy Standards.

Section 14. Return and Destruction of PHI. At termination of the Agreement, Contractor shall either return or destroy all PHI received from, or created or received by Contractor on behalf of, HHSC that Contractor still maintains in any form. Contractor shall further not retain any copies of such information in any form. In the event such return or destruction is not feasible, Contractor shall (1) provide an explanation in writing to HHSC as to why such return or destruction is not feasible; (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 15. Termination for Violation. Notwithstanding any other provisions of the Agreement to the contrary, if HHSC determines that Contractor 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 Standards or the Security Standards.

"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, which:

- (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 Standards" shall mean the Standards 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 Right and Privacy Act, as amended, 20 U.S.C. § 1232g, or records described in 20 U.S.C. § 1232g(a)(4)(B)(iv).

"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 Standards" shall mean the Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and C, as amended from time to time.