ADDENDUM A

DHHS HIPAA BUSINESS ASSOCIATE AGREEMENT PROVISIONS

RFP 6303 Z1

1. BUSINESS ASSOCIATE. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR § 160.103, and in reference to the party in this Contract, shall mean Contractor.

2. COVERED ENTITY. "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 Contract, shall mean DHHS.

3. HIPAA RULES. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

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

5. OTHER TERMS. The following terms shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Subcontractor, Unsecured Protected Health Information, and Use.

6. THE CONTRACTOR shall do the following:
   - 6.1. Not use or disclose Protected Health Information other than as permitted or required by this Contract or as required by law. Contractor may use Protected Health Information for the purposes of managing its internal business processes relating to its functions and performance under this Contract. Use or disclosure must be consistent with DHHS' minimum necessary policies and procedures.
   - 6.2. Implement and maintain appropriate administrative, physical, and technical safeguards to prevent access to and the unauthorized use and disclosure of Protected Health Information. Comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information, to prevent use or disclosure of Protected Health Information other than as provided for in this Contract and assess potential risks and vulnerabilities to the individual health data in its care and custody and develop, implement, and maintain reasonable security measures.
   - 6.3. To the extent Contractor is to carry out one or more of the DHHS' obligations under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to DHHS in the performance of such obligations. Contractor may not use or disclosure Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by DHHS.
   - 6.4. In accordance with 45 CFR §§ 164.502(E)(1)(ii) and 164.308(b)(2), if applicable, ensure that any agents and subcontractors that create, receive, maintain, or transmit Protected Health Information received from DHHS, or created by or received from the Contractor on behalf of DHHS, agree in writing to the same restrictions, conditions, and requirements relating to the confidentiality, care, custody, and minimum use of Protected Health Information that apply to the Contractor with respect to such information.
   - 6.5. Obtain reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and 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 Contractor of any instances of which it is aware that the confidentiality of the information has been breached.
   - 6.6. Contractor shall maintain and make available within fifteen (15) days in a commonly used electronic format:
     - 6.6.1. Protected Health Information to DHHS as necessary to satisfy DHHS' obligations under 45 CFR § 164.524;

6.6.2. Any amendment(s) to Protected Health Information as directed or agreed to by DHHS pursuant to 45 CFR § 164.526, or take other measures as necessary to satisfy DHHS' obligations under 45 CFR § 164.526;

6.6.3. The information required to provide an accounting of disclosures to DHHS as necessary to satisfy DHHS' obligations under 45 CFR § 164.528.

6.7. Make its internal practices, books, and records relating to the use and disclosure of Protected Heath Information received from, or created or received by the Contractor on behalf of the DHHS available to the Secretary or DHHS for purposes of determining compliance with the HIPAA rules. Contractor shall provide DHHS with copies of the information it has made available to the Secretary at the same time as it was made available to the Secretary.

6.8. Report to DHHS within fifteen (15) days of which the Contractor becomes aware, any unauthorized use or disclosure of Protected Health Information made in violation of this Contract, or the HIPAA rules, including any security incident that may put electronic Protected Health Information at risk. Contractor shall, as instructed by DHHS, take immediate steps to mitigate any harmful effect of such unauthorized disclosure of Protected Health Information pursuant to the conditions of this Contract through the preparation and completion of a written Corrective Action Plan subject to the review and approval by DHHS. The Contractor shall be responsible for all breach notifications in accordance with HIPAA rules and regulations and all costs associated with security incident investigations and breach notification procedures.

6.9. Business Associate shall indemnify, defend, and hold harmless DHHS for any financial loss as a result of claims brought by third parties and which are caused by the failure of Contractor, its officers, directors, agents or subcontractors to comply with the terms of this Contract or for penalties imposed by the HHS Office of Civil Rights for any violations of the HIPAA rules caused by Contractor, its officers, directors, agents or subcontractors. Additionally, Contractor shall indemnify DHHS for any time and expenses it may incur from breach notifications that are necessary under the HIPAA Breach Notification Rule, which are caused by a failure of Contractor, its officers, directors, agents or subcontractors to comply with the terms of this Contract.

7. TERMINATION.

7.1. DHHS may immediately terminate this Contract and any and all associated contracts if DHHS determines that the Contractor has violated a material term of this Contract.

7.2. Within thirty (30) days of expiration or termination of this Contract, or as agreed, unless Contractor requests and DHHS authorizes a longer period of time, Contractor shall return or at the written direction of DHHS destroy all Protected Health Information received from DHHS (or created or received by Contractor on behalf of DHHS) that Contractor still maintains in any form and retain no copies of such Protected Health Information. Contractor shall provide a written certification to DHHS that all such Protected Health Information has been returned or destroyed (if so instructed), whichever is deemed appropriate. If such return or destruction is determined by DHHS to be infeasible, Contractor shall use such Protected Health Information only for purposes that makes such return or destruction infeasible and the provisions of this Contract shall survive with respect to such Protected Health Information.

7.3. The obligations of the Contractor under the Termination Section shall survive the termination of this Contract.