



*Delaware Health
And Social Services*

DIVISION OF MANAGEMENT SERVICES

PROCUREMENT

DATE: June 15, 2015

HSS-15-031

Background Check Center Maintenance

for

Division of Long Term Care Resident Protection

Date Due: July 6th, 2015
By 11:00 am Local Time

ADDENDUM # 1 – Appendix B - IT Requirements

PLEASE NOTE:

THE ATTACHED SHEETS HEREBY BECOME A PART OF THE ABOVE MENTIONED RFP.

Kieran Mohammed
Procurement Administrator

Tom Murray
Division Contact

APPENDIX B – Information Technology Related Requirements

1.1 Support/Technical Environment

The three groups responsible for the development and operation of the automated systems that support the Division are described below. These three groups will be responsible for review and approval of all project deliverables, invoices and milestone payments. IRM will serve as the liaison with DTI (see below). The selected contractor will coordinate efforts for this project with the IRM Applications Manager and DLTCRP Administration and Business staff.

1.1.1 Information Resource Management (IRM)

The IRM Applications Manager will report to the Director of Information Resource Management and have a dotted line to DTI's Director of Major Projects. The IRM Applications Manager will monitor the project budget in coordination with the Division, DTI, and OMB. The IRM unit is responsible for providing DHSS divisions with direct programming support of automated systems, as well as consulting support and management of automated systems software, vendors and development projects. IRM consists of an Applications Development, Technology Planning, Base Technology, Telecommunications, Security, and Help Desk support group all who participate in all phases of the project lifecycle as appropriate.

1.1.2 Department of Technology and Information (DTI)

DTI is a separate cabinet level agency responsible for running the State of Delaware's mainframe computer operations, wide area data network, and setting and enforcing statewide IT policy and standards. DTI as a separate state agency does not fall under the authority of DHSS. However, the IRM Applications Manager has a dotted line to DTI's Director of Major Projects and is required to work with DTI groups throughout all phases of the project lifecycle, review project deliverables, and oversee the project budget. DTI is responsible for supplying mainframe and Wide Area Network (WAN) systems support to DHSS as well as other state agencies. Additionally, DTI provides 24x7 data center operations support. DTI provides state agencies with technical consultant services.

1.1.3 Division Staff

Division staff typically work with IRM to translate business needs into IT requirements and vice versa. This is a critical function that ensures that division business requirements are properly communicated to technical staff and that division program staff understand IT policies and standards as they relate to the project. This group works closely with IRM and vendor staff on all technical aspects of the project, including RFP, business case process, vendor negotiations, deliverable review and signoff, through testing, implementation, and post-implementation support.

1.2 Resource Availability

Test systems availability will be scheduled in concert with other development staff. DTI has mainframe systems support staff on site from 7:00 AM to 4:30 PM. DTI Operations staff are on site 24x7. IRM applications, telecommunications and HelpDesk staff are on site from 8:00 AM to 4:30 PM on State business days. The State network is very stable and unscheduled downtime is minimal. Given that the network is an essential state resource, any reported problems have a very high priority and are dealt with immediately. Biggs Data Center power is conditioned and outside supply fluctuations can

trigger a switch to automatic local power generation capability. The State has audio and video-conferencing capabilities as well in specific on-site locations for remote meeting participation. Remote connectivity through SSL-VPN is available for offsite work for contracted staff that must access, update or maintain servers and/or applications in the DMZ.

1.3 Implementation

Production implementation is normally an IRM responsibility. Depending on circumstances, IRM may require participation of contractor staff. The state will be primarily responsible for post implementation administration, and the system resides at the Biggs Data Center.

1.4 Staffing

Demonstrated experience is critical in ensuring project success. Contractor will propose and supply resumes for the following key positions including:

- Project Coordinator
- Senior Developers
- Technical Analysts (i.e. DBA, SE, etc.)
- Documentation Specialists

Other positions may be proposed at the contractor's discretion. One person may be proposed to fill more than one role.

1.4.1 Offsite Project Work

The State expects most of this project work to be done offsite, but only within the United States. For offsite work, the State requires strong management of the resources and assigned tasks; adequate, timely and accurate communications and completion of assigned work by specified deadlines. This is important to any offsite relationship.

1.5 Requirement to Comply With HIPAA Regulations and Standards

The selected vendor must certify compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations and requirements as described in Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160, 162 and 164 along with the updated ARRA and HITECH act provisions, as well as all HIPAA requirements related to privacy, security, transaction code sets (where applicable) and medical provider enumeration.

The selected vendor is required to customize/develop the system in accordance with HIPAA requirements, implement the system in accordance with HIPAA requirements and, where the vendor will operate and maintain the system, operate and maintain the system in compliance with HIPAA requirements.

HIPAA requirements also apply to entities with which State data is shared. If this data is covered by HIPAA, then a Business Associates Agreement (BAA) or contractual agreement specifying vendor responsibility for protecting and securing this data must be signed by both parties to ensure that this data is adequately secured according to State and DHSS policies and standards. This agreement/contract must be in force prior to testing, production implementation, or data exchange. A copy of the BAA contractual agreement to be used is attached as Appendix E of the RFP.

In the proposal, contractor will explain their understanding of the HIPAA regulations and their impact on this project especially in the area of security.

1.6 Requirement to Comply with State Policies and Standards

The proposed solution must be fully compatible with the Department of Health and Social Services' technical environment. Vendor solutions that are not fully compliant with State standards may be disallowed.

The Information Technology Publications web page <http://www.dhss.delaware.gov/dhss/dms/itpubs.html> has links to the DHSS and DTI policies and standards and other documentation. See the "Supportive Documentation for Bidding on Proposals" section.

- Please review the IAS documents referenced on this page. IAS is the Integrated Authorization System which is a department mechanism for tracking authorized systems users. Bidders will comply specifically with these requirements. MCI is the Master Client Index which is required for all systems identifying DHSS clients, but the DLTCRP Background Check Center system does not currently identify DHSS clients so MCI is not currently applicable to that system.

The DTI Systems Architecture Standard contains information confidential to the State and is not available from the internet. However, DTI has set up an email address which will automatically send a response with this document attached. The email address is sysarch@lists.state.de.us

The application must be maintained with at least 3 tiers, with the tiers configured and secured as in the sample diagram included in the DHSS Information Technology Environment Standards. Please see State of Delaware Systems Architecture Standard (instructions above) and DHSS Information Technology Environment Standards

http://www.dhss.delaware.gov/dhss/dms/irm/files/dhss_it_environment.pdf for more information.

All components of the proposed solution, including third party software and hardware, are required to adhere to the policies and standards described above, as modified from time to time during the term of the contract resulting from this RFP, including any links or documents found at the above referenced web sites. Any proposed exceptions must be addressed in the Transmittal Letter RFP response.

1.6.1 Authorizations

Contractor staff will be required to fill out DTI's Acceptable Use Policy, Biggs Data Center User Authorization Form, and the Biggs Data Center Non-Disclosure Agreement for necessary authorizations before starting work.

All contractor staff working on this project will be subject to a Criminal Background Check (CBC). The contractor will be solely responsible for the cost the CBC. DHSS will review the CBC results. DHSS at their sole discretion may request that a contractor staff member be replaced if their CBC result is unsatisfactory.

Contractor staff are required to request their own criminal history. For privacy reasons, the SBI and FBI will not mail the results to anyone except the requestor, so the results must be delivered to the DHSS Security Manager at the Biggs Data Center in a sealed envelope. Costs will be borne by the contractor. Below are instructions for obtaining the required criminal background checks with fingerprinting done at a Delaware State Police location. An alternate procedure is available for contractor staff to be fingerprinted at any local police station within the United States.

1. Visit one of the Delaware State Police locations listed on the next page. Note: For the New Castle and Sussex locations, appointments may take up to six weeks to schedule.
2. Complete a SBI Personal Criminal History authorization form.
3. Present valid government-issued photo identification, such as a driver's license.
4. The State fee is \$45 and the Federal check fee is \$10, payable by cash or debit/credit card. (No personal checks).
5. The State Police will require you to fill out an FBI fingerprint card, which they will return to you after you have completed the fingerprint process.
6. Complete and sign the FBI Applicant Information Form to request the national record check. The form can be found on-line at <http://www.fbi.gov/about-us/cjis/background-checks/applicant-information-form>

7. Mail the Cover Letter and fingerprint card, along with an \$18 processing fee, payable by money order, certified check, or credit card. The FBI turnaround time is 3-6 weeks.
8. When you receive your reports at your home address, DO NOT OPEN THE ENVELOPES. If you break the seal on the envelopes, you will be responsible to go through the process again at your own expense.
9. Either hand-deliver or mail the SEALED FBI and SBI envelopes to:

DHSS Security Manager
 1901 N Dupont Highway
 Biggs Data Center
 New Castle, DE 19720

Mark envelopes as CONFIDENTIAL.

The results of the criminal background check will be reviewed and kept completely confidential. The total cost is \$73.

New Castle County	Kent County (Primary Facility)	Sussex County
<p>State Police Troop 2</p> <p>100 LaGrange Ave Newark, DE 19702 (Between Rts. 72 and 896 on Rt. 40)</p> <p>** By appointment only To schedule an appointment: Phone: 302-739-2528 or Toll Free 1-800-464-4357</p>	<p>State Bureau of Identification</p> <p>655 Bay Road Blue Hen Mall and Corporate Center Suite 1B Dover, DE 19903 Customer Service: 302-739-5871</p> <p>** Walk-ins accepted Hours of Operation Monday 9AM – 7PM Tuesday – Friday 9AM – 3PM</p>	<p>State Police Troop 4</p> <p>S DuPont Hwy & Shortly Rd Georgetown, DE 19947 (Across from DeIDOT & State Service Center)</p> <p>** By appointment only (every other Wednesday) To schedule an appointment: Phone: 302-739-2528 or Toll Free 1-800-464-4357</p>

1.6.2 Architecture Requirements

Securing and protecting data is critical to the State. This protection is required for data whether hosted **onsite or offsite**. As such it is required that the vendor include in the response to this section a proposed architectural diagram(s) in Visio format demonstrating how State data would be secured at their offsite location.

1.6.2.1 Security

Computer, network, and information security is of paramount concern for the State of Delaware and the Department of Technology and Information. The State wants to ensure that computer/network hardware and software does not compromise the security of its IT infrastructure. The SANS Institute and the FBI have released a document describing the Top 20 Internet Security Threats. The document is available at www.sans.org/top20.htm for your review. The Contractor is guaranteeing that any systems or software provided by the Contractor are free of the vulnerabilities listed in that document.

1.6.2.2 Cyber Security Liability

It shall be the duty of the Vendor to assure that all products of its effort do not cause, directly or indirectly, any unauthorized acquisition of data that compromises the security, confidentiality, or integrity of information maintained by the State of Delaware. Vendor's agreement shall not limit or modify liability for information security breaches, and Vendor shall indemnify and hold harmless the State, its agents and employees, from any and all liability, suits, actions or claims, together with all reasonable costs and expenses (including attorneys' fees) arising out of such breaches. In addition to all rights and remedies available to it in law or in equity, the State shall subtract from any payment made to Vendor all damages, costs and expenses caused by such information security breaches that have not been previously paid to Vendor.

1.6.2.3 Standard Practices

The contractor(s) shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services furnished to the State. The contractor(s) shall follow practices consistent with generally accepted professional and technical policies and standards.

HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is entered into this ____ day of _____, 20____ ("**Effective Date**"), by and between [Vendor Name] ("**Business Associate**"), and the State of Delaware, Department of [Agency/Division Name] ("**Covered Entity**") (collectively, the "**Parties**").

RECITALS

WHEREAS, The Parties have entered, and may in the future enter, into one or more arrangements or agreements (the "Agreement") which require the Business Associate to perform functions or activities on behalf of, or services for, Covered Entity or a Covered Entity Affiliate ("CE Affiliate") that involve the use or disclosure of Protected Health Information ("PHI") that is subject to the final federal Privacy, Security, Breach Notification and Enforcement Rules (collectively the "HIPAA Rules") issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (the Act including the HIPAA rules shall be referred to as "HIPAA") and the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), as each is amended from

time to time. The purpose of this BAA is to set forth the obligations of the Parties with respect to such PHI.

WHEREAS, Business Associate provides [professional services] for Covered Entity pursuant to a contract dated [redacted], 201[redacted] and such other engagements as shall be entered into between the parties in the future in which Covered Entity discloses certain Protected Health Information (“PHI”) to Business Associate (collectively, the “Master Agreement”);

WHEREAS, Business Associate, in the course of providing services to Covered Entity, may have access to PHI and may be deemed a business associate for certain purposes under HIPAA;

WHEREAS, the Parties contemplate that Business Associate may obtain PHI, with Covered Entity’s knowledge and consent, from certain other business associates of Covered Entity that may possess such PHI; and

WHEREAS, Business Associate and Covered Entity are entering into this BAA to set forth Business Associate’s obligations with respect to its handling of the PHI, whether such PHI was obtained from another business associate of Covered Entity or directly from Covered Entity;

NOW, THEREFORE, for mutual consideration, the sufficiency and delivery of which is acknowledged by the Parties, and upon the premises and covenants set forth herein, the Parties agree as follows:

1. Definitions. Unless otherwise defined herein, capitalized terms used in this BAA shall have the meanings ascribed to them in HIPAA or the Master Agreement between Covered Entity and Business Associate, as applicable.

2. Obligations and Activities of Business Associate. To the extent that Business Associate is provided with or creates any PHI on behalf of Covered Entity and is acting as a business associate of Covered Entity, Business Associate agrees to comply with the provisions of HIPAA applicable to business associates, and in doing so, represents and warrants as follows:

(a) **Use or Disclosure.** Business Associate agrees to not use or disclose PHI other than as set forth in this BAA, the Master Agreement, or as required by law.

(b) **Specific Use of Disclosure.** Except as otherwise limited by this BAA, Business Associate may:

(i) use or disclose PHI to perform data aggregation and other services required under the Master Agreement to assist Covered Entity in its operations, as long as such use or disclosure would not violate HIPAA if done by Covered Entity, or HIPAA permits such use or disclosure by a business associate;

(ii) use or disclose PHI for the proper management and administration of Business Associate or to carry out Business Associate’s legal responsibilities, provided that with respect to disclosure of PHI, such disclosure is required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached; and

(iii) de-identify PHI and maintain such de-identified PHI indefinitely, notwithstanding Section 4 of this Agreement, provided that all identifiers are destroyed or returned in accordance with the Privacy Rule.

(c) **Minimum Necessary.** Business Associate agrees to take reasonable efforts to limit requests for, or uses and disclosures of, PHI to the extent practical, a limited data set, otherwise to the minimum necessary to accomplish the intended request, use, or disclosure.

(d) **Safeguards.** Business Associate shall establish appropriate safeguards, consistent with HIPAA, that are reasonable and necessary to prevent any use or disclosure of PHI not expressly authorized by this BAA.

(i) To the extent that Business Associate creates, receives, maintains, or transmits Electronic PHI, Business Associate agrees to establish administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity, as required by the Privacy Rule and Security Rule.

(ii) The safeguards established by Business Associate shall include securing PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity in accordance with the standards set forth in HITECH Act §13402(h) and any guidance issued thereunder.

(iii) Business Associate agrees to provide Covered Entity with such written documentation concerning safeguards as Covered Entity may reasonably request from time to time.

(e) **Agents and Subcontractors.** Business Associate agrees to obtain written assurances that any agents, including subcontractors, to whom it provides PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, agree to the same restrictions and conditions that apply to Business Associate with respect to such PHI, including the requirement that it agree to implement reasonable and appropriate safeguards to protect Electronic PHI that is disclosed to it by Business Associate. To the extent permitted by law, Business Associate shall be fully liable to Covered Entity for any and all acts, failures, or omissions of Business Associate's agents and subcontractors in any breach of their subcontracts or assurances to Business Associate as though they were Business Associate's own acts, failures, or omissions.

(f) **Reporting.** Within five (5) business days of discovery by Business Associate, Business Associate agrees to notify Covered Entity in writing of any use or disclosure of, or Security Incident involving, PHI, including any Breach of Unsecured PHI, not provided for by this BAA or the Master Agreement, of which Business Associate may become aware.

(i) In the notice provided to Covered Entity by Business Associate regarding unauthorized uses and/or disclosures of PHI, Business Associate shall describe the remedial or proposed mitigation efforts required under Section 2(g) of this BAA.

(ii) Specifically with respect to reporting a Breach of Unsecured PHI, Business Associate agrees to must include the identity of the individual(s) whose Unsecured PHI was Breached in the written notice provided to Covered Entity, and any additional information required by HIPAA.

(ii) Business Associate agrees to cooperate with Covered Entity upon report of any such Breach so that Covered Entity may provide the individual(s) affected by such Breach with proper notice as required by HIPAA.

(g) **Mitigation.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate resulting from a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA or the Master Agreement.

(h) **Audits and Inspections.** Business Associate agrees to make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI available to the Secretary, in a time and manner mutually agreed to by the Parties or designated by the Secretary, for purposes of the Secretary determining the Covered Entity's compliance with HIPAA.

(i) **Accounting.** Business Associate agrees to document and report to Covered Entity, within fourteen (14) days, Business Associate's disclosures of PHI so Covered Entity can comply with its accounting of disclosure obligations in accordance with 45 C.F.R. §164.528 and any subsequent regulations issued thereunder. Business Associate agrees to maintain electronic records of all such disclosures for a minimum of six (6) calendar years.

(j) **Designated Record Set.** While the Parties do not intend for Business Associate to maintain any PHI in a designated record set, to the extent that Business Associate does maintain any PHI in a designated record set, Business Associate agrees to make available to Covered Entity PHI within fourteen (14) days:

(i) for Covered Entity to comply with its access obligations in accordance with 45 C.F.R. §164.524 and any subsequent regulations issued thereunder; and

(ii) for amendment upon Covered Entity's request and incorporate any amendments to PHI as may be required for Covered Entity comply with its amendment obligations in accordance with 45 C.F.R. §164.526 and any subsequent guidance.

(k) **HITECH Compliance Dates.** Business Associate agrees to comply with the HITECH Act provisions expressly addressed, or incorporated by reference, in this BAA as of the effective dates of applicability and enforcement established by the HITECH Act and any subsequent regulations issued thereunder.

3. Obligations of Covered Entity.

(a) Covered Entity agrees to notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices in accordance with 45 C.F.R. §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) Covered Entity agrees to notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, including disclosure of data to insurers and health plans when the patient pays for medical services in full and requests that such notification not be made, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity agrees to notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d) Covered Entity agrees to limit its use, disclosure, and requests of PHI under this BAA to a limited data set or, if needed by Covered Entity, to the minimum necessary PHI to accomplish the intended purpose of such use, disclosure, or request.

4. Term and Termination.

(a) **Term.** This BAA shall become effective upon the Effective Date and, unless otherwise terminated as provided herein, shall have a term that shall run concurrently with that of the last expiration date or termination of the Master Agreement.

(b) **Termination Upon Breach.**

(i) Without limiting the termination rights of the Parties pursuant to the Master Agreement, upon either Party's knowledge of a material breach by the other Party to this BAA, the breaching Party shall notify the non-breaching Party of such breach and the breaching party shall have fourteen (14) days from the date of notification to the non-breaching party to cure such breach. In the event that such breach is not cured, or cure is infeasible, the non-breaching party shall have the right to immediately terminate this BAA and those portions of the Master Agreement that involve the disclosure to Business Associate of PHI, or, if nonseverable, the Master Agreement.

(c) **Termination by Either Party.** Either Party may terminate this BAA upon provision of thirty (30) days' prior written notice.

(d) **Effect of Termination.**

(i) To the extent feasible, upon termination of this BAA or the Master Agreement for any reason, Business Associate agrees, and shall cause any subcontractors or agents to return or destroy and retain no copies of all PHI received from, or created or received by Business Associate on behalf of, Covered Entity. Business Associate agrees to complete such return or destruction as promptly as possible and verify in writing within thirty (30) days of the termination of this BAA to Covered Entity that such return or destruction has been completed.

(ii) If not feasible, Business Associate agrees to provide Covered Entity notification of the conditions that make return or destruction of PHI not feasible. Upon notice to Covered Entity that return or destruction of PHI is not feasible, Business Associate agrees to extend the protections of this BAA to such PHI for as long as Business Associate maintains such PHI.

(iii) Without limiting the foregoing, Business Associate may retain copies of PHI in its workpapers related to the services provided in the Master Agreement to meet its professional obligations.

5. **Miscellaneous.**

(a) **Regulatory References.** A reference in this BAA to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

(b) **Amendment.** The Parties acknowledge that the provisions of this BAA are designed to comply with HIPAA and agree to take such action as is necessary to amend this BAA from time to time as is necessary for Covered Entity to comply with the requirements of HIPAA. Regardless of the execution of a formal amendment of this BAA, the BAA shall be deemed amended to permit the Covered Entity and Business Associate to comply with HIPAA.

(c) **Method of Providing Notice.** Any notice required to be given pursuant to the terms and provisions of this BAA shall be in writing and may be either personally delivered or sent by registered or certified mail in the United States Postal Service, Return Receipt Requested, postage prepaid, addressed to each Party at the addresses

listed in the Master Agreement currently in effect between Covered Entity and Business Associate. Any such notice shall be deemed to have been given if mailed as provided herein, as of the date mailed.

(d) **Parties Bound.** This BAA shall inure to the benefit of and be binding upon the Parties hereto and their respective legal representatives, successors, and assigns. Business Associate may not assign or subcontract the rights or obligations under this BAA without the express written consent of Covered Entity. Covered Entity may assign its rights and obligations under this BAA to any successor or affiliated entity.

(e) **No Waiver.** No provision of this BAA or any breach thereof shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

(f) **Effect on Master Agreement.** This BAA together with the Master Agreement constitutes the complete agreement between the Parties and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. In the event of any conflict between the terms of this BAA and the terms of the Master Agreement, the terms of this BAA shall control unless the terms of such Master Agreement are stricter, as determined by Covered Entity, with respect to PHI and comply with HIPAA, or the Parties specifically otherwise agree in writing. No oral modification or waiver of any of the provisions of this BAA shall be binding on either party. No obligation on either party to enter into any transaction is to be implied from the execution or delivery of this BAA.

(g) **Interpretation.** Any ambiguity in this BAA shall be resolved to permit the Covered Entity to comply with HIPAA and any subsequent guidance.

(h) **No Third Party Rights.** Except as stated herein, the terms of this BAA are not intended nor should they be construed to grant any rights, remedies, obligations, or liabilities whatsoever to parties other than Business Associate and Covered Entity and their respective successors or assigns.

(i) **Applicable Law.** This BAA shall be governed under the laws of the State of Delaware, without regard to choice of law principles, and the Delaware courts shall have sole and exclusive jurisdiction over any dispute arising under this Agreement.

(j) **Judicial and Administrative Proceedings.** In the event that Business Associate receives a subpoena, court or administrative order, or other discovery request or mandate for release of PHI, Business Associate agrees to collaborate with Covered Entity with respect to Business Associate's response to such request. Business Associate shall notify Covered Entity within seven (7) days of receipt of such request or mandate.

(k) **Transmitting Electronic PHI.** Electronic PHI transmitted or otherwise transferred from between Covered Entity and Business Associate must be encrypted by a process that renders the Electronic PHI unusable, unreadable, or indecipherable to unauthorized individuals within the meaning of HITECH Act § 13402 and any implementing guidance including, but not limited to, 42 C.F.R. § 164.402.

6. IN WITNESS WHEREOF, the Parties hereto have executed this BAA to be effective on the date set forth above.

Covered Entity

Business Associate

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____