ENTERPRISE BUSINESS ASSOCIATE AGREEMENT

Standard Terms and Conditions

This Enterprise Business Associate Agreement ("BAA"), Contract ID# XXXX, is between the entity (“Company”) and Supplier Name ("Supplier"), a (jurisdiction) whose address is Supplier’s address (insert address)

Whereas, the Office for Civil Rights, Department of Health and Human Services, has published final regulations fully implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act ("HITECH Act") (42 U.S.C. §17934 et. seq.), and also making various technical, conforming and other amendments to the HIPAA rules, being entitled "Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Non-Discrimination Act; Other Modifications to the HIPAA Rules" (the "Final Rule") (published at 78 F.R. 5566 (January 25, 2013));

Whereas, this BAA incorporates the various amendments, technical and conforming changes to HIPAA implemented by the Final Rule;

Whereas, pursuant to this BAA Supplier may function as a business associate or as a business associate sub-contractor to one or more covered entities;

Whereas, the parties to this BAA agree that the obligations herein govern the exchange of all Protected Health Information ("PHI") and personally identifiable information ("PII") as set forth below. Anytime PHI or PII is exchanged, this BAA shall be automatically incorporated into the agreement entered into between Company and Supplier governing such services (in their cumulative total, "Agreements").

Whereas, both parties to the BAA and Agreements desire to continue conducting business with each other and to remain fully compliant with the law; and

Now, therefore, in consideration of their mutual promises and other valuable consideration, the sufficiency of which is acknowledged by the parties, the parties hereby agree to the foregoing and as follows:

Section 1: Applicable Law and Policy.

1.1. Supplier acknowledges that it performs services or assists Company in the performance of a function or service that involves the use or disclosure of PHI, and therefore the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), and stricter state and federal laws, as applicable, require that the PHI an PII be protected from inappropriate uses or disclosures.

1.2. Supplier acknowledges that under HIPAA, its use and disclosure of PHI must be in compliance with the terms of this BAA and 45 C.F.R. §164.504(e).

1.3. Capitalized terms not otherwise defined shall have the meaning as set forth in HIPAA.

Section 2: Use and Disclosure of PHI and PII.

2.1. PHI and PII, in electronic form or otherwise, may be used or disclosed only when required by law or as necessary to enable Supplier to satisfy the obligations and to perform the functions, activities, services and operations to which Supplier is contractually obligated by Company. Supplier shall not and shall ensure that its directors, officers, employees, contractors and agents, do not, use PHI or PII received from Company in any manner that would constitute a violation of applicable law.

2.2. Supplier shall not and shall ensure that its directors, officers, employees, contractors, and agents do not disclose PHI or PII received from Company in any manner that would constitute a violation of applicable law if disclosed by Company. Supplier may disclose PHI or PII(a) as permitted and pursuant to the requirements of this BAA or (b) as required by law.

2.3. To the extent Supplier discloses PHI or PII to a third party, Supplier must obtain, prior to making any such disclosure:

2.3.1. Reasonable assurances evidenced by written contract from such third party that PHI or PII will be held confidential and safeguarded consistent with the terms of this BAA, and only used or further disclosed for the purpose for which Supplier disclosed it to the third party or as required by law; and

2.3.2. An agreement from such third party to immediately notify Supplier (who will in turn notify Company in accordance with Section 4 of this BAA) of any:

2.3.2.1. Unauthorized access, use or disclosure of PHI;

2.3.2.1.1. Security Incident as defined in 45 C.F.R. §164.304 and further explained in Section 4.2 of this BAA; and

2.3.2.1.2. Breaches of the confidentiality of the PHI, as Breach is defined by 45 C.F.R §164.402,

to the extent such third party has discovered such unauthorized access, use or disclosure of PHI, Security Incident or Breach.

2.3.2.2. Unauthorized access use or disclosure of PII.

2.4. Supplier shall utilize a Limited Data Set, if practicable, for all uses, disclosures or requests of PHI. Otherwise, any uses or disclosures of PHI shall be limited to the "Minimum Necessary," as defined in 45 C.F.R. §514(d) and any further guidance that may be issued by the Department of Health and Human Services. Supplier acknowledges its obligation under 45 C.F.R. §164.502(b) to determine what constitutes the minimum necessary to accomplish the intended purposes of any disclosure of PHI.

2.5. Supplier shall not send PHI or PII to an offshore location or allow access to PHI or PII at an offshore location without Company's prior written consent.

Section 3: Safeguards Against Misuse of Information.

3.1. Supplier agrees that it will implement all appropriate safeguards, including at least the minimum provisions set forth in Company 's Supplier Privacy and Information Security Requirements document, the terms of which are incorporated into this BAA by reference, to prevent the access, use or disclosure of PHI or PII other than pursuant to the terms and conditions of this BAA. Such safeguards include administrative, physical, and technical safeguards that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of the electronic PHI and PII that it creates, receives, maintains, or transmits on behalf of Company, as required by 45 CFR Part 160 and Subparts A and C of Part 164 ("Security Rule"). Supplier shall implement all Security Rule provisions and requirements as more fully described in the Final Rule and the associated implementing regulations, as may be amended from time to time.

3.2. Supplier will require any of its subcontractors and agents, to which Supplier is expressly permitted in writing by Company in advance to disclose PHI, to provide satisfactory assurances, as evidenced by written contract in accordance with 45 C.F.R. §164.504(e)(1)(i), that such subcontractor or agent will comply with the same privacy and security safeguard obligations with respect to PHI and PII that are applicable to Supplier under this BAA, including but not limited to the provisions set forth in Section 2.3.

Section 4: Reporting of Disclosures of PHI, Breaches & Security Incidents.

4.1. Supplier shall report to Company any access, use or disclosure of PHI or PII in violation of this BAA, including any breach of unsecured PHI and any successful Security Incident (as defined in 45 C.F.R. §164.304) (collectively, "Incident") of which it becomes aware.

4.1.1. Supplier shall provide notice of any Incident within twenty-four (24) hours of Supplier's knowledge of the Incident (the "24 Hour Notice"). The 24 Hour Notice shall be made to Company by sending an email to Company's Contract Administrator or other appropriate contact as determined by Company. The 24 Hour Notice shall include as much information about the Incident set forth in Paragraph 4.3 below as is known at the time;

4.1.2. In the event the 24 Hour Notice does not provide all of the information contained in Paragraph 4.3 below, then Supplier shall provide written supplemental incident report(s) with all of the information set forth in Paragraph 4.3 below (the "Supplemental Incident Report(s)") by sending an email to Company's Contract Administrator or other appropriate contact as determined by Company. The Supplemental Incident Report(s) must be provided as promptly as possible, but in no event more than 24 hours after learning of the new information, on a rolling basis after Supplier learns of the additional information.

4.2. The HIPAA Security Rule defines a "Security Incident" as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system, involving PHI that is created, received, maintained or transmitted by or on behalf of Company in electronic form (45 C.F.R. §164.304). Supplier shall also notify Company of attempts to bypass Supplier's electronic security mechanisms.

4.2.1. Both parties recognize, however, that the significant number of meaningless attempts to, without authorization, access, use, disclose, modify or destroy PHI in Supplier's information systems could make a real-

time reporting requirement formidable for both parties. Both parties believe that the Security Rule notice requirements are met by instituting a process by which:

4.2.1.1. Supplier discloses to Company the rate and types of attempted incidents that are occurring at the time this Business Associate Agreement is signed;

4.2.1.2. Supplier monitors the rate and nature of such attempts over time; and

4.2.1.3. Supplier reports to Company any substantive changes to the rate or nature of such attempts that could adversely affect Company directly or indirectly.

4.2.2. The following are illustrative of unsuccessful Security Incidents when they do not result in unauthorized access, use, disclosure, modification, or destruction of PHI or interference with an information system:

4.2.2.1. Pings on a firewall;

4.2.2.2. Port scans;

4.2.2.3. Attempts to log on to a system or enter a database with an invalid password or username; and

4.2.2.4. Malware (e.g., worms, viruses).

4.2.3. If Supplier observes through ongoing monitoring successful Security Incidents that extend beyond these routine, unsuccessful attempts in such a way that they could impact the Confidentiality, Integrity or Availability of PHI, Supplier agrees to promptly notify Company.

4.3. If Supplier is required to report (a) a Security Incident, (b) a data Breach, or (c) any other non-permitted access, use or disclosure of PHI or PII, such report must be sent to the Company HIPAA Privacy and Security Official and include at a minimum:

4.3.1. The date and time the event occurred and the date it was discovered;

4.3.2. A complete description of the PHI or PII accessed, used or disclosed;

4.3.3. A complete description of the event, its cause, and the effect it had on our systems and data. This should include the names of the affected systems, servers, programs, etc.;

4.3.4. Contact information for communications regarding the event;

4.3.5. A description of the initial mitigation steps taken to contain the event and an assessment of the level of compromise to our data incurred by Supplier;

4.3.6. A description of the plan to correct the compromises to our data and to prevent reoccurrences of the event in the future; and

4.3.7. Such other information, including a written report, as Company may reasonably request.

4.4. Supplier shall comply with applicable laws that require notification to individuals in the event of an unauthorized access to or release of PII or PHI, as defined by applicable state or federal law, or other event requiring notification ("Notification Event"), whether such Notification Event was the responsibility of Supplier or a third party to which Supplier disclosed PII or PHI. When notification to individuals is required by law or determined by Company, in its sole discretion, to be necessary under this BAA, whether such Notification Event was the responsibility of Supplier or a third party to which Supplier disclosed PII or PHI, Supplier shall coordinate with Company to (a) investigate the Notification Event, (b) inform all affected individuals and (c) mitigate the Notification Event. At Company's sole discretion, mitigation includes but is not limited to securing credit monitoring or protection services for affected individuals for a period of no less than twenty four (24) months as determined by Company. Supplier shall be responsible for any and all costs associated with responding to and mitigating such Notification Events, including but not limited to mailing costs, personnel costs, attorney fees, credit monitoring costs, and other related expenses or costs. Notwithstanding any limitation of liability provided in this or any other agreements, including statements of work, between the parties, Supplier agrees to indemnify, hold harmless, and defend Company, or any of its covered entity business partners in such case Company functions as a business associate, from and against any and all claims, damages, fines, costs or other related harm associated with Notification Events.

4.5. Supplier agrees to indemnify and hold Company, or, in such case that Company functions as a business associate to one or more covered entities, each and every of its covered entity business partners harmless from any and all liability, damages, costs (including reasonable attorney fees and costs) and expenses imposed upon or asserted against Company, or any of its covered entity business partners arising out of any claims, demands, awards, settlements, fines or judgments relating to Supplier's access, use or disclosure of PHI or PII contrary to the provisions of this BAA.

Section 5: Agreements by Third Parties.

5.1. Supplier shall enter into an agreement with any agent or subcontractor that will have access to PHI or PII that is received from, or created or received by Supplier on behalf of, Company pursuant to which such agent or

subcontractor agrees to be bound by the same restrictions, terms, and conditions that apply to Supplier pursuant to this BAA, including those safeguards described in Section 3 above.

Section 6: Access to Information.

6.1. Within five (5) business days of a request by Company for access to PHI about an individual, Supplier shall make available to Company such PHI for so long as such information is maintained by Supplier.

6.2. In the event any individual requests access to PHI directly from Supplier, Supplier shall within two (2) business days forward such request to Company. Any denials of access to the PHI requested shall be the responsibility of Company . Supplier will make available to Company or at Company 's direction, to the individual, such PHI in a manner consistent with 45 C.F.R. §164.524, so that Company may meet its access obligations under 45 C.F.R. §164.524.

6.3. To the extent Supplier maintains electronic PHI in a Designated Record Set, with respect to such electronic PHI of an individual, Supplier agrees that the individual, and Company on behalf of the individual, shall have a right to obtain an electronic copy of such information in the form and format requested by the Individual or Company , if such electronic PHI is readily reproducible in the form and format so requested. If the information is not readily reproducible in the form or format requested by either the individual or Company , Supplier shall make the information available in a readable electronic format as mutually agreed to by the individual, Supplier and Company . Supplier also agrees to transmit an electronic copy of electronic PHI information directly to a person or entity designated by the individual, or designated by Company on behalf of the individual, provided the direction is in writing, and is clear, conspicuous and specific. Supplier shall provide a copy of any request by an individual for access to electronic PHI to Company within two (2) business days of its receipt of the request.

Section 7: Availability of PHI for Amendment.

7.1. Within ten (10) business days of receipt of a request from Company for the amendment of an individual's PHI, Supplier shall provide such information to Company for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

Section 8: Accounting of Disclosures.

8.1. Within ten (10) business days of notice by Company to Supplier that it has received a request for an accounting of disclosures of PHI regarding an individual during the six (6) years prior to the date on which the accounting was requested, Supplier shall make available to Company such information as is in Supplier's possession and is required for Company to make the accounting required by 45 C.F.R. §164.528.

8.2. To the extent Supplier maintains PHI as an Electronic Health Record, Supplier acknowledges that the exception at 45 C.F.R. §164.528(a)(1)(i) not requiring disclosures for the purpose of carrying out Treatment, Payment, and Healthcare Operations is inapplicable and that these disclosures must be tracked for three years.

8.3. For disclosures that it is required to track, at a minimum, Supplier shall provide Company with the following information:

- 8.3.1. the date of the disclosure;
- 8.3.2. the name of the entity or person who received the PHI, and if known, the address of such entity or person;
- 8.3.3. a brief description of the PHI disclosed;
- 8.3.4. a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure; and
- 8.3.5. Supplier further shall provide any additional information to the extent required by the HIPAA or the Final Rule, and any accompanying regulations.

8.4. In the event the request for an accounting is delivered directly to Supplier, Supplier shall within two (2) business days forward such request to Company . It shall be Company's responsibility to prepare and deliver any such accounting requested.

8.5. Supplier hereby agrees to implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section.

Section 9: Restriction Agreements and Confidential Communications.

9.1. Supplier shall comply with any agreement that Company makes that either (a) restricts use or disclosure of PHI pursuant to 45 C.F.R. §164.522(a), or (b) requires Confidential Communication about PHI pursuant to 45 C.F.R. §164.522(b), provided Company notifies Supplier of the restriction or Confidential Communication obligations. Company shall promptly notify Supplier in writing of the termination of any such restriction agreement or Confidential Communication requirement, and with respect to termination of such restriction agreement, instruct Supplier whether any PHI will remain subject to the terms of the restriction agreement.

Section 10: Restriction on Remuneration for EHR, PHI, and Marketing.

10.1. Supplier shall neither directly nor indirectly receive remuneration in exchange for any PHI except as permitted by 45 C.F.R. §164.502(5)(ii)(B). In addition, Supplier shall neither directly nor indirectly receive remuneration in connection with a communication to purchase or use a product except as permitted by 45 C.F.R. §164.508(a)(3) and with Company 's express prior written permission.

Section 11: Fundraising.

11.1. Supplier shall not make any fundraising communication to a Company member.

Section 12: Availability of Books and Records.

12.1. Supplier hereby agrees to make its internal practices, books, and records relating to the use and disclosure of PHI or PII received from, or created or received by Supplier on behalf of, Company available to; (i) the Secretary of the Department of Health and Human Services for purposes of determining Company's and Supplier's compliance with the Standards for Privacy and Security of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164 ("Privacy and Security Standards"); and (ii) to Company for its purposes in responding to a formal investigation or enforcement action by the Secretary of Health and Human Services, Office for Civil Right, or, alternatively, the Centers for Medicare and Medicaid Services, or for the purposes of evaluating and/or responding to a compliance review performed, conducted, overseen, or managed, in whole or in part, by the aforementioned governmental agencies.

Section 13: Termination and Return of Records.

13.1. Upon termination of any Agreements, Supplier shall, if feasible, return or destroy all PHI or PII received from, or created or received by the Supplier on behalf of, Company that Supplier still maintains in any form and retain no copies of such information.

13.1.1. Supplier will require any subcontractor or agent, to which Supplier has disclosed PHI or PII, to, if feasible, return the same to Supplier (so that Supplier may return it to Company) or destroy the same in whatever form or medium received from Supplier, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of the PHI or PII, and certify to Supplier that all such information has been returned or destroyed.

13.1.2. Supplier will complete these obligations as promptly as possible, but not later than forty-five (45) business days following the effective date of the termination or other conclusion of any Agreement, and shall provide an attestation to that all PHI and PII provided under this BAA has been returned or destroyed.

13.2. If such return or destruction of PHI or PII by Supplier or their subcontractor or agent is not feasible, Supplier and their subcontractors and agents shall limit their further use or disclosure of such information to the purposes that make return or destruction of the PHI infeasible.

13.3. If such return or destruction of PHI or PII by Supplier or their subcontractor or agent is not feasible, the obligation to protect the privacy and safeguard the security of PHI and PII as specified in this BAA will be continuous and survive termination or other conclusion of this BAA or any other Agreements, including statements of work, entered into between Supplier and Company. Moreover, Supplier shall, on an annual basis, provide an attestation to that it and its subcontractors and agents are in compliance with the BAA (including the attached Enterprise Information Security Requirements Document) and shall permit to audit its books, records and operations to determine compliance with Supplier's obligations under the BAA.

13.4. If Company determines that Supplier has violated the provisions of this BAA, Company may immediately terminate this BAA and any other Agreements, including statements of work, entered into between the parties that require Supplier to access, use or disclose PHI or PII.

Section 14: Compliance with Transaction Standards.

14.1. ICD-10 Code Sets

14.1.1. If Supplier's services or products use or require the use of Code Sets, as defined in HIPAA, then Supplier shall utilize the International Classification of Diseases, 10th Revision, Clinical Modification ("ICD-10-CM") for diagnosis coding, and the International Classification of Diseases, 10th Revision, Procedural Coding System ("ICD-10-PCS") for inpatient hospital procedure coding for all services or products for which Supplier is contractually obligated to provide to Company .

14.1.2. Company is not responsible for any additional services, programming, processing, testing, or other implementation costs incurred by Supplier to implement ICD-10-CM and ICD-10-PCS, as these are the responsibility of Supplier. Company shall have no obligation to reimburse Supplier for any costs related to testing, implementation, or remediation associated with Supplier's implementation of ICD-10-CM and ICD-10-PCS.

14.1.3. If Company reasonably determines that Supplier's products or services have not implemented or addressed the applicable provisions of the HIPAA Code Set Standards or the provisions set forth in this Section, and provided Supplier does not remediate such issue within thirty (30) calendar days of notification, or as otherwise agreed to by Company in writing, Company may withhold payments to Supplier until such time as the issue is remediated to Company 's reasonable satisfaction.

14.2. Compliance with HIPAA Standard Transactions

14.2.1. If Supplier (or its agent or subcontractor) performs or conducts (in whole or in part) electronic Transactions on behalf of Company for which the Department of Health and Human Services ("DHHS") has established Standards (collectively referred to as "Transactions"), Supplier shall comply (and shall require any subcontractor or agent involved in the acceptance or processing of such Transactions to comply) with the requirements of the Transaction Rule, 45 C.F.R. Part 162, including any Implementation Guide specifications incorporated into the Rule by reference.

14.2.2. Supplier will not enter into, or permit its subcontractors or agents to enter into, any Trading Partner Agreement in connection with the conduct of Standard Transactions on behalf of Company that:

14.2.2.1. Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;

14.2.2.2. Adds any data element or segment to the maximum defined data set;

14.2.2.3. Uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification or is not in the Standard Transaction's implementation specification; or

14.2.2.4. Changes the meaning or intent of the Standard Transaction's implementation specification.

14.2.3. Supplier acknowledges that DHHS published modifications to the HIPAA Standard Transaction Rules on January 16, 2009, replacing current versions of the standards with versions 5010, D.0, and 3.0, effective January 1, 2012.

14.2.3.1. Version 5010 is the new version of the X12 standards for HIPAA transactions;

14.2.3.2. Version D.0 is the new version of the National Council for Prescription Drug Program ("NCPDP") standards for pharmacy and supplier transactions; and

14.2.3.3. Version 3.0 is a new NCPDP standard for Medicaid pharmacy subrogation.

14.2.4. Supplier acknowledges that DHHS published modifications to the HIPAA Code Set Rules on January 16, 2009, effective on October 1, 2014. Supplier further acknowledges that DHHS modified the standard medical data code sets for coding diagnoses and inpatient hospital procedures by adopting the International Classification of Diseases, 10th Revision, Clinical Modification ("ICD-10-CM") for diagnosis coding, and the International Classification of Diseases, 10th Revision, Procedural Coding System ("ICD-10-PCS") for inpatient hospital procedure coding. These new codes replace the current International Classification of Diseases, 9th Revision, Clinical Modification, Volumes 1 and 2, and the International Classification of Diseases, 9th Revision, Clinical Modification, Volume 3 for diagnosis and procedure codes, respectively.

14.2.5. Company is not responsible for any additional services, programming, processing, testing, or other implementation costs incurred by Supplier to attain compliance with the HIPAA Standard Transaction Rules V5010, ICD-10-CM, and ICD-10-PCS, as these are the responsibility of Supplier. Company shall have no obligation to reimburse Supplier for any costs related to testing, implementation, or remediation associated

with Supplier's HIPAA Standard Transaction Rule V4010A1, HIPAA Standard Transaction Rule V5010, ICD-10-CM, or ICD-10-PCS compliance.

14.2.6. Upon Company's request, Supplier shall conduct end-to-end or other Transactions and Code Set compliance testing and certify to Company that Supplier complies with the applicable laws.

14.2.7. Upon Company's request, Supplier shall provide a copy of its compliance certification (for both levels 1 and 2) from an approved third-party certification company. Absent Company's reasonable determination of Transactions or Code Set compliance issues, such requests shall be limited to once per year.

14.2.8. Upon Company's written notice of a Transactions or Code Set compliance issue, Supplier and Company, as applicable, shall investigate and remediate such issue within a mutually agreed upon timeframe. Remediation shall include any testing activities that may be required to validate compliance. If Company and Supplier disagree on the interpretation of the standard, regulation or rules, the parties agree to submit a request for clarification and / or interpretation to an industry recognized or designated body, including but not limited to, the Accredited Standards Committee (ASC) X12 or Workgroup for Electronic Data Interchange (WEDI).

14.2.9. If Company reasonably determines that Supplier is not in compliance with the Transactions or Code Set rules or the provisions set forth in this Section, and provided Supplier does not remediate such compliance issue within thirty (30) calendar days of notification, or as otherwise agreed to by Company in writing, Company may withhold payments to Supplier until such time as the compliance issue is remediated to Company 's reasonable satisfaction. To the extent Company is fined, assessed a penalty, or is otherwise held responsible for any Transactions or Code Set compliance issue and such non-compliance is related to Supplier's actions or omissions, Supplier shall reimburse Company for all such fines, penalties, or other associated costs imposed on Company.

Section 15: Amendment to Agreement.

15.1. Upon the effective date of any amendment to the Privacy Standards or the Security Rule or the effective date of any other final regulations with respect to PHI or other state or federal laws applicable to PHI or PII, this BAA will automatically be amended so that the obligations they impose on Supplier shall remain in compliance with such regulations.

Section 16: Conflicts.

16.1. The terms and conditions of this BAA supersede and override any other Health Insurance Portability and Accountability Act of 1996 (HIPAA) terms and conditions contained within any agreements, including statements of work, entered into by Company and Supplier, including but not limited to, any agreements with its subsidiaries, affiliates, parent companies, officers, directors, employees, contractors, and/or agents.

Section 17: Disclaimer of Agency Relationship.

17.1. Nothing in this BAA or any services or similar agreement between the parties shall give rise to an agency relationship as between Supplier and BCSBM and the parties expressly disclaim the existence of any such relationship.

Section 18: Compliance with Other Laws Governing PHI or PII

18.1. Supplier, its agents, employees, and subcontractors agree to comply with all state and federal laws, statutes, regulations, rulings, or enactments of any governmental authority governing the use and disclosure of PHI or PII, including, without limitation, each individual state's data breach security laws and the Confidentiality of Substance Use Disorder Patient Records Rule, 45 C.F.R. Part 2.

Signatures

The above BAA is agreed to by both parties as witnessed by their respective signatures below. By signing this BAA, the signatory certifies and warrants that he or she has the actual authority to bind Supplier to it for all of Supplier's agreements and statements of work with Company. Notwithstanding any statement to the contrary in any other agreements and statements of work between Supplier and Company, this BAA is effective when signed by the Company Procurement Agent and Supplier.

COMPANY	**SUPPLIER NAME**
By: _____ (signature)	By: _____ (signature)
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date:_____