Business Associate Agreement and Qualified Organization Agreement

THIS HIPAA BUSINESS ASSOCIATE AGREEMENT (this "Agreement") is by and between **Hudson Partnership CMO** ("Covered Entity") and **[Enter Name]** ("Business Associate") (hereinafter, Covered Entity and Business Associate are, at times, referred to individually each as a "Party" and together as "the Parties").

RECITALS:

WHEREAS, Covered Entity has engaged Business Associate for the purpose of performing certain functions and engaging in certain activities *for and on behalf of* Covered Entity, as set forth in the underlying agreement between the Parties (hereinafter, the "Services Agreement") with regard to **(describe service/function)**

WHEREAS, in connection with such BA Services, it may become necessary for Covered Entity to disclose information to Business Associate, some of which may constitute protected health information ("PHI"), including electronic protected health information ("e-PHI") (PHI and e-PHI are, collectively, referred to hereinafter as "Covered Entity's PHI") as defined below;

WHEREAS, the Parties intend to protect the privacy and provide for the security of Covered Entity's PHI in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (the "HIPAA Statute"), and its related "Privacy Rule" (45 CFR Part 164 Subpart E) and "Security Rule" (45 CFR Part 164 Subpart C) (collectively, the Privacy Rule, Security Rule and HIPAA Statute are, hereinafter, referred to as "**HIPAA**"), all as amended by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Statute") and its regulations promulgated thereunder (collectively, the "HITECH Rules," and together with the HITECH Statute, referred to hereinafter simply as "**HITECH**"), as well in compliance with other applicable federal or state laws concerning the privacy and security of health information;

WHEREAS, Covered Entity operates a federally funded part 2 program in New Jersey that must comply with the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations, 42 USC §290dd-2 and 42 CFR Part 2 (collectively, "Part 2");

WHEREAS, Business Associate is also a Qualified Service Organization (QSO) under Part 2 and must agree to certain mandatory provisions regarding the use and disclosure of substance abuse treatment information; and

WHEREAS, the Parties desire to set forth the terms and conditions pursuant to which Protected Health Information, provided to Business Associate by Covered Entity ("Protected Health Information"), will be handled between themselves and third parties.

NOW THEREFORE, in consideration of the foregoing, the mutual representations, covenants and agreements set forth below and in the underlying Services Agreement, and for other good and valuable consideration, the Parties, intending to be legally bound, hereby agree as follows:

TERMS:

A. Definitions. Any terms not otherwise specifically defined in this Agreement shall have the meanings ascribed to them in HIPAA and HITECH.

B. Uses and Disclosures of Covered Entity's PHI.

1) ***Permitted Uses and Disclosures.*** Business Associate may use and/or disclose Covered Entity's PHI made available by Covered Entity, or created or obtained by Business Associate for or on behalf of Covered Entity as follows:

a) to furnish or perform the BA Services set forth in the Services Agreement, as permitted by and in accordance with this Agreement, HIPAA, HITECH and all other applicable federal or state laws. Business Associate may not use or disclose Covered Entity's PHI in a manner that would violate HIPAA and HITECH if done by Covered Entity, this BA Addendum, or applicable law;

b) to use and or disclose only the minimum necessary amount of Covered Entity's PHI needed for Business Associate to perform the BA Services, as consistent with Covered Entity's minimum necessary policies and procedures, and including in accordance with any minimum necessary standards and guidance released by the U.S. Department of Health & Human Services (HHS) pursuant to the HITECH Act;

c) for internal management and administration purposes of Business Associate only if ***use*** of Covered Entity's PHI is necessary for Business Associate to perform internal management and administration functions, or to carry out its own internal legal responsibilities;

d) for the internal management and administration purposes of Business Associate only if ***disclosure*** of Covered Entity's PHI: (1) the disclosure is required by law, or (2) Business Associate obtains from such third party recipient written assurances: (a) that such recipient will hold Covered Entity's PHI confidential and (b) that such recipient will notify the Business Associate, without unreasonable delay, of any instances of which such recipient becomes aware of a Breach that compromises the confidentiality of Covered Entity's PHI. **Notwithstanding the foregoing, Business Associate, shall NOT, under any circumstances, disclose Covered Entity's PHI to any third party not within the borders and jurisdiction of the United States of America without the prior written consent of the Covered Entity, which may be withheld in Covered Entity's sole and unfettered discretion;]**

e) for data aggregation for and on behalf of Covered Entity in accordance with 164.504(e)(2)(i)(B);

f) to the extent Business Associate is to carry out a function or obligation of Covered Entity with respect to the Privacy Rule, comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation.

2) ***Business Associates' Agents.*** Business Associate shall ensure that any agent to whom it provides Covered Entity's PHI agrees to implement reasonable and appropriate security measures to protect such PHI. The agent/subcontractor will agree to comply with 42 C.F.R. Part 2 and HIPAA, and if Business Associate learns of a pattern or practice by the agent/subcontractor that is a material breach of the contract with Business Associate, to take reasonable steps to cure the breach or terminate the contract, if feasible.

3) ***HIPAA Authorization.*** Business Associate shall not, except as provided in this Agreement and permitted or required under HIPAA and HITECH, use in any other manner or disclose to any other person or entity Covered Entity's PHI without first obtaining a HIPAA-compliant authorization ("HIPAA Authorization") from the individual about whom the information pertains, including, but not limited to, whenever Covered Entity would be required to do so under applicable state law, including but not limited to the Community Mental Health Services Act rules (N.J.A.C. 10:37 et seq.) the New Jersey AIDS Assistance Act (N.J.S.A. 26:5C-1 et seq.), restrictions governing venereal diseases (N.J.S.A. 26:4-41 et seq.), the New Jersey Genetic Privacy Act (N.J.S.A. 10:5-43 et seq.), New Jersey laws governing emancipated minor's rights regarding health care services (N.J.S.A. 9:2-4.2 et seq.), or any other applicable State or federal law. Business Associate must retain a copy of any such HIPAA Authorization obtained for six (6) years, and make copies available to Covered Entity.

4) ***QUALIFIED SERVICE ORGANIZATION AGREEMENT.*** Covered Entity and Business Associate hereby agree that this Agreement constitutes a Qualified Service Organization Agreement ("QSOA") as required by 42 CFR Part 2. Accordingly, information obtained by Business Associate relating to individuals who may have been diagnosed as needing, or who have received, substance use disorder treatment services shall be maintained and used only for the purposes intended under this Agreement and in conformity with all applicable provisions of 42 USC § 290dd-2 and the underlying federal regulations, 42 C.F.R. Part 2. This includes but is not limited to resisting any efforts in judicial proceedings to obtain access to the Protected Health Information, pursuant to 42 C.F.R. Part 2. Accordingly, except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity provided that such use or disclosure would not violate the Confidentiality or Privacy Rules if done by Covered Entity.

5) ***Prohibited Uses and Disclosures.***

a) *Prohibition on "Sale" of PHI and "Marketing"*. Business Associate shall not directly or indirectly accept remuneration in exchange for using or disclosing any of Covered Entity's PHI, including in de-identified form,

except Business Associate may accept such remuneration from Covered Entity in exchange for services or functions performed pursuant to this Agreement. Business Associate shall not use or disclose Covered Entity's PHI for marketing except for or on behalf of Covered Entity with Covered Entity's express written consent and the individual's Authorization.

b) *All Other Uses Strictly Prohibited*. Business Associate is strictly prohibited from using or disclosing Covered Entity's PH in any other manner except as expressly permitted under this Agreement, **including, but not limited to, manipulating or otherwise converting such information to de-identified format, even if any such use or disclosure is otherwise permitted under HIPAA and or HITECH, unless Covered Entity agrees in advance in writing.]**

C. Security Safeguards.

1) ***General***. Business Associate shall have in place reasonable and appropriate safeguards to provide for the security of Covered Entity's PHI and prevent use or disclosure of Covered Entity's PHI other than as provided for by this Agreement in accordance with the HIPAA Security Rule, including but not limited to those administrative, technical and physical safeguard Standards as set forth in § 164.308, § 164.310, § 164.312 of the Security Rule.

a) *Compliance with Security Rule*. Business Associate shall comply with the requirements of the Security Rule at all times with respect to Covered Entity's PHI.

b) *Administrative & Other Safeguards*. Business Associate shall implement and maintain a **written** security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of Business Associate's operations and the nature and scope of its activities and as reasonable necessary for Business Associate to comply with applicable provisions of the HIPAA Security Rule, including but not limited to all "Required" and "Addressable" Implementation Specifications.

c) *Documentation*. Business Associate shall maintain written or electronic policies and procedures developed to comply with the HIPAA Security Rule. If any action, activity or assessment is required under the HIPAA Security Rule to be documented, Business Associate shall maintain a written (or electronic) record of the same, and retain a copy and make it available to Covered Entity upon request for a period of six (6) years from the date of its creation, or the date when it last was in effect, whichever is later.

d) *HHS Guidance*. Business Associate shall implement and comply with all requirements set forth in any guidance concerning business associate

compliance with the Security Rule that may be issued by HHS pursuant to the HITECH Act, Part 2, or HIPAA.

2) Security Breach Notification.

a) ***General***. Business Associate shall comply with the standards and requirements under the Breach Notification Laws, which for purposes of this Agreement include, collectively, the provisions relating to breach as set forth in the HITECH Statute and its related Rules for Breach Notification for Unsecured Protected Health Information (45 CFR Parts 160 and 164), and the New Jersey Identity Theft Prevention Act (NJITPA), and its related regulations, as may be amended from time to time, and may be applicable to Business Associate.

b) ***Encryption***. Business Associate shall encrypt Covered Entity's PHI when maintained by Business Associate (i.e., "at rest") and when transmitted by Business Associate (i.e., "in transit") to render it unusable, unreadable and indecipherable, including any and all of Covered Entity's PHI that Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses for or on behalf of Covered Entity pursuant to this Agreement. If the Parties otherwise mutually agree that it is not reasonable or possible for Business Associate to encrypt Covered Entity's PHI, then Business Associate shall implement reasonable alternative security methods, as agreed to by Covered Entity in its sole and unfettered discretion, to safeguard Covered Entity's PHI.

c) ***BA's Obligations in the Event of a Security Incident or Breach.***

i. Reporting Security Incidents and Breaches. Business Associate shall promptly report to Covered Entity's Privacy Officer and/or Security Officer, or their respective designee, either in person or by telephone at a number to be provided by Covered Entity, any incident, including any Breach or Security Incident, as such terms are defined by HIPAA, that has or may result in the unauthorized use or disclosure of Covered Entity's PHI, and in no case later than **seventy-two (72) hours** from the date of actual or constructive discovery by Business Associate.

ii. Presumption of Breach. In accordance with 45 C.F.R. § 164.402, *any acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a Breach unless a low probability exists that the PHI has been compromised*. For purposes of this Addendum, a Breach shall be deemed "discovered" by Business Associate as of the first day on which such Breach is actually known to any person, other than the individual committing the Breach, that is an employee, officer, or other agent of Business Associate, or if such Breach should

reasonably have been known to Business Associate to have occurred, including but not limited to notification provided to Business Associate by a subcontractor of a Breach. Business Associate shall take all commercially reasonable steps (e.g., audits; hotlines; technological tools etc.) to allow it to discover Breaches and Security Incidents involving Covered Entity's PHI.

iii. No Delay for Risk Assessment. Business Associate shall not delay Breach or Security Incident reporting on the basis of there being a pending determination of whether the incident may result in a "low probability" that Covered Entity's PHI was compromised or other harm or misuse assessment which may be required under the Breach Notification Laws. Covered Entity has the sole and unfettered right to make any and all final risk assessment determinations, and Business Associate shall cooperate with investigations if requested by Covered Entity in order for Covered Entity to comply with its obligations under HITECH.

iv. Assistance and Cooperation. Business Associate shall provide Covered Entity with such information as may be required for Covered Entity to appropriately determine whether an incident is a Security Incident or Breach, and provide such notification as may be required under the Breach Notification Laws. Business Associate agrees to assist and cooperate with Covered Entity as needed for Covered Entity and Business Associate to fully comply with the Breach Notification Laws. If Business Associate is the direct or indirect cause of a Breach of Covered Entity's PHI, including any of Business Associate's employees, owners, directors, agents, independent contractors, or affiliates, Business Associate shall provide Covered Entity, at Business Associate's sole cost, administrative support and other resources as may be requested by Covered Entity in order to furnish written notices to individuals affected by the Breach and otherwise comply with the Breach Notification Laws. In the event that Business Associate does not provide such requested assistance and resources in a timely manner, as determined by Covered Entity in its sole and unfettered discretion, then Business Associate shall reimburse Covered Entity for all reasonable and actual costs and expenses (e.g., postage; supplies; administrative staff time, etc.) incurred by Covered Entity in its efforts to comply with the Breach Notification Laws.]

v. Indemnification for Failures to Discover or Report Breaches. Business Associate shall defend, indemnify and hold harmless Covered Entity and each of its officers, directors, employees and agents ("Covered Entity Affiliates") from and against any and all penalties, claims, losses, liabilities, damages, costs and expenses

(including reasonable attorneys' fees and expenses) incurred by Covered Entity or any Covered Entity Affiliates arising out of or in connection with Business Associate's negligent failure to (a) discover a Breach, (b) timely notify Covered Entity of a Breach that is known or should have been known to Business Associate or (c) otherwise comply with Business Associate's obligations under the Breach Notification Laws and this Agreement.

D. Amendment of PHI**.** Business Associate shall make Covered Entity's PHI available to Covered Entity as may be required for Covered Entity to fulfill its obligations to respond under §164.526 of the Privacy Rule to an individual's request for amendment of his or her protected health information. Business Associate agrees to incorporate any amendments, as directed by Covered Entity, into copies of Covered Entity's PHI maintained by Business Associate.

E. Restrictions. Business Associate shall implement any restrictions on use or disclosure of Covered Entity's PHI that Covered Entity has agreed to and provided notice to Business Associate of, including but not limited to any restriction for disclosure of PHI to a health plan where the Individual paid in full and out-of-pocket and such disclosure would be for the sole purpose of payment or health care operations purposes.

F. Access Rights of Individual**.** Business Associate agrees to make Covered Entity's PHI available to Covered Entity as may be required for Covered Entity to fulfill its obligations under § 164.524 of the Privacy Rule to provide an Individual with access or a copy of such individual's PHI, including but not limited to making available PHI maintained in an electronic designated record set in an electronic form and format as requested by the Individual, if readily producible. Business Associate's compliance with such "access rights" requirements shall be at Business Associate's cost. Notwithstanding the forgoing, Business Associate may, if Covered Entity agrees, to charge a "copy/labor fee" to the individual as otherwise permitted under HIPAA, HITECH and State law.

G. Accounting of Disclosures. Business Associate shall maintain and make available documentation as required under § 164.528 of the Privacy Rule to allow Covered Entity to respond to an individual's request for an accounting of disclosures (AOD) by Business Associate. Business Associate shall provide such information as may be necessary in order for Covered Entity to respond to an individual's request for an accounting of disclosures as required by 45 C.F.R. § 164.528, as modified by HITECH and its implementing accounting of disclosure rules and regulations.

H. Business Associate's Subcontractors**.** Business Associate expressly acknowledges that HITECH makes directly applicable to Business Associate and its subcontractors certain provisions of the HIPAA Privacy Rule and the Security Rule, and that such subcontractors may be considered "business associates" in their own respect with regard to PHI that they may create, receive, maintain or transmit for or on behalf of Business Associate. Business Associate hereby agrees to:

1) Ensure that any subcontractor that creates, receives, maintains or transmits Covered Entity's PHI for or on behalf of Business Associate enters into a written HIPAA Business Associate Agreement that complies with the requirements of §164.314(a) and §164.508(e), as applicable;

2) Ensure that each such subcontractor is notified and made aware that it is directly responsible for complying with applicable provisions of the HIPAA Privacy and Security Rules, including 42 CFR Part 2, as a Business Associate as a result of entering into such HIPAA Business Associate Agreement with respect to Covered Entity's PHI;

3) Ensure that each HIPAA Business Associate Agreement shall contain the same restrictions and conditions which apply to Business Associate with respect to Covered Entity's PHI; and

I. Training. Business Associate agrees to require its directors, officers, employees, and agents that have access to Covered Entity's PHI to: (a) undergo HIPAA and HITECH-related training and education; and (b) agree to abide by Business Associate's specific responsibilities and obligations with respect to accessing and using Covered Entity's PHI under this Agreement.

J. Books and Records. Except for information accorded legal protection as privileged or confidential information, each Party agrees to make its internal practices, books and records relating to the use and disclosure of Covered Entity's PHI available if access to such information is necessary for the Secretary of HHS to determine Covered Entity's compliance with HIPAA and HITECH.

K. State Law. The Parties agree that if any provision or requirement concerning privacy or security of Covered Entity's PHI under New Jersey law is more stringent or provides individuals with more rights regarding their protected health information than a similar provision or requirement under HITECH or HIPAA, such state law shall be followed.

L. Termination.

1) ***Noncompliance.*** If Covered Entity notifies Business Associate regarding an activity or practice that constitutes a material breach or violation of an obligation under this Agreement, HIPAA or HITECH, and Business Associate does not take reasonable steps to or otherwise does not successfully cure the breach or end the violation, as applicable, within a reasonable timeframe as determined by Covered Entity, Covered Entity may terminate this Agreement and Business Associate's authority to access, use and/or maintain possession of Covered Entity's PHI.

2) ***Judicial or Administrative Proceedings.*** Covered Entity may terminate this Agreement immediately if: i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA or HITECH, or other criminal law or, ii) a finding or stipulation that Business Associate has violated any standard or

requirement of HIPAA, HITECH or other law is made in any administrative or civil proceeding in which Business Associate has been joined.

3) ***Return of Covered Entity's PHI.*** Upon termination of the underlying Services Agreement or this Agreement, Business Associate shall return to Covered Entity and/or destroy all of Covered Entity's PHI that Business Associate or any of its subcontractors still maintains in any form, and Business Associate and its subcontractors shall retain no copies of Covered Entity's PHI. If return or destruction is not feasible, Business Associate agrees to continue to extend the protections of this Agreement to such information, and limit further use of Covered Entity's PHI to those purposes that make the return or destruction of such PHI infeasible, and similarly require any of its subcontractors to extend such protections and limit further use/disclosure of Covered Entity's PHI, as applicable.

M. Assistance in Litigation or Administrative Proceedings. Each Party agrees to reasonably assist the other in the performance of its obligations under this Agreement including, if necessary, to testify as witnesses in the event that any litigation or administrative proceedings are commenced against a Party based upon a claimed violation of HIPAA, HITECH, except where the other Party, or its subcontractor, employee or agent may be named as an adverse Party.

N. Amendment. The Parties acknowledge that state and federal laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Agreement may be necessary to address such developments. Upon either Party's request, the Parties agree to in good faith promptly enter into negotiations concerning the terms of an amendment to this Agreement embodying written assurances consistent with the standards and requirements of HIPAA, Part 2, and HITECH or other applicable laws. Either Party may terminate this Agreement and Business Associate's right to continued access to or possession of the PHI upon **30 days written notice** in the event that a Party, or any of its agents and subcontractors: (i) does not promptly enter into negotiations to amend this Agreement when requested by the other Party pursuant to this paragraph or (ii) does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI sufficient to satisfy the standards and requirements of HIPAA, Part 2, and HITECH.

O. Independent Contractor. Nothing contained herein shall be deemed or construed by the Parties hereto or by any third party as creating the relationship of employer and employee, principal and agent, partners, joint venturers, or any similar relationship. Covered Entity and Business Associate expressly acknowledge and agree that Business Associate is an independent contractor, and not an agent of Covered Entity, under federal agency law or otherwise.

P. No Waiver. Neither the failure or any delay on the part of a Party to exercise any right, remedy, power or privilege under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise of any right, remedy, power or privilege with respect

to any occurrence be construed as a waiver of such right, remedy, power or privilege with respect to any other occurrence.

Q. Governing Law. This Agreement shall be construed in accordance with and governed by the laws of New Jersey.

R. Binding Effect. This Agreement shall inure to the benefit of, and be binding upon each Party hereto and their respective successors and assigns.

S. Notices. All notices to be made under this Agreement shall be given in writing and shall be deemed to have been duly given if personally delivered or sent by confirmed facsimile transmission, e-mail, certified or registered mail, return recipe requested, to the other Party at the address set forth in the underlying Services Agreement.

T. Modification**.** This Agreement may be amended, superseded, terminated or extended, and the terms hereof may be waived, only by a writing signed by the Parties.

U. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, such provision shall be deemed severed from this Agreement, and the remainder of the provisions will remain in full force and effect.

V. Interpretation. The Parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and HITECH. If any provision of this Agreement conflicts with a provision in the underlying Services Agreement, the terms of this Agreement will control. The use of headings in this Agreement are for convenience only and shall not affect the interpretation hereof.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement effective as of the date of signature below (the "Effective Date"):

FOR COVERED ENTITY:	**FOR BUSINESS ASSOCIATE:**
By: _____	By: _____
Print Name:	Print Name:
Title:	Title:
Date:	Date: