State of New Jersey
DEPARTMENT OF HEALTH

BUSINESS ASSOCIATE AGREEMENT

Between

The New Jersey Department of Health
(Enter Division)

AND

(Add Vendor)

This Business Associate Agreement (the "Agreement"), is entered into by and between _____, (the "Business Associate") and the New Jersey Department of Health, ("NJDOH") ADD DIVISION, (the "Covered Entity") (collectively the "Parties").

WHEREAS, the Parties have entered into the following agreement: ADD NAME/REFERENCE OF UNDERLYING K/MOA ("the Underlying Agreement), executed on ADD DATE and

WHEREAS, the Business Associate may use, disclose, create, receive, maintain or transmit protected health information ("PHI") on behalf of the Covered Entity in connection with Business Associate's performance of its obligations under the above-referenced Underlying Agreement; and

WHEREAS, the Parties intend to ensure the confidentiality, privacy and security of PHI as required by Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 and the regulations promulgated thereunder by the U.S. Department of Health (the HIPAA Regulations), as updated by the Human Services and the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted under Title XII of the American Recovery and Reinvestment Act of 2009, and other applicable laws; and

WHEREAS, there are no underlying agreements associated with this Agreement other than the above-referenced Underlying Agreement.

NOW THEREFORE, the parties hereby agree to the following.

A. Definitions

Unless otherwise provided for in this Agreement, terms used in this Agreement shall have the same meaning as set for the in HIPAA, HITECH, and the underlying regulations, including but not limited to the following: Availability, Breach, Confidentiality, Data Aggregation, Designated Record Set, Health Care Operations, Individual, Integrity, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, and Use. Specific definitions are as follows:

a. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and 164, Subparts A and E.

b. "Security Rule" shall mean the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160, 162 and 164.

B. Obligations and Activities of Business Associate

1. **Security Safeguards**. The Business Associate shall use appropriate safeguards and comply with Subpart C of 45 CFR Part 164, Security Standards to prevent the use or disclosure of Electronic Protected Health Information (ePHI), other than as authorized under this Agreement, and maintain a reasonable and appropriate privacy and security program that includes appropriate administrative, technical, organizational and physical safeguards to protect the confidentiality, integrity and availability of PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity.

2. **Breach of Security and Privacy.** The Business Associate agrees to notify the Covered Entity's Privacy Officer, as noted in Section H.45, to promptly notify Covered Entity of any Security Incident involving PHI of which it becomes aware and cooperate with Covered Entity in the investigation. Business Associate will report attempted but unsuccessful Security Incidents that do not result in any unauthorized access, use, disclosure, modification or destruction of PHI, or interference with an information system at Covered Entity's request. In addition, to the extent the information is available, the following information, to the extent available, shall be provided to the Covered Entity as soon as possible, but no later than fourteen (14) days after the Business Associate becomes aware of such security incident:

    a. Specify the nature of the unauthorized access, use or disclosure;
    b. Identify the PHI accessed, used or disclosed
    c. Identify the cause the security incident
    d. Identify the recipient(s) of the PHI
    e. Identify what corrective action took place or will take place to prevent further breaches
    f. Explain what was done or will be done to mitigate the harmful effect
    g. Provide any other relevant information Covered Entity may need about a breach.

3. **Mitigation**. The Business Associate agrees to take prompt corrective action to mitigate any harmful effect of any use or disclosure of PHI, or security incident that is known to the Business Associate.

4. **Agents.** The Business Associate agrees to ensure that any officer, employee, contractor, subcontractor or agent to whom it provides PHI, which was received, maintained, created, used or transmitted by the Business Associate on behalf of the Covered Entity agrees in writing to the same restrictions and conditions that apply through this Agreement to the Business Associate with respect to such PHI.

5. **Right of Access to PHI**. **Right of Access to PHI**. The Business Associate agrees to make available PHI in a designated record set maintained by the Business Associate or its agents or subcontractors to the Covered Entity as necessary to satisfy the covered entity's obligations under 45 CFR 164.524 within ten days (10) days of the date of any such request. Business Associates agrees to forward all requests made directly to the Business Associate from individuals seeking access to PHI.

6. **Amendments.** The Business Associate agrees to make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526 within thirty (30) days of such a request, or take other measures as necessary to satisfy the Covered Entity's obligations under 45 CFR 164.526. The Business Associate shall provide written confirmation of the amendment(s) to the Covered Entity. Business Associates agrees to forward all requests made directly to the Business Associate from individuals seeking amendments to PHI.

7. **Access to books and records.** The Business Associate agrees to make its privacy and security program, its internal practices, books and records relating to the use, disclosure and security of PHI under this Agreement and the Underlying Agreement available to the Covered Entity within thirty (30) days of the date of such request, or to the Secretary of the U.S. Department of Health & Human Services, in a time and manner designated by the Secretary.

8. **Accounting of Disclosures.** The Business Associate agrees to maintain and make available the information and/or documentation required to provide an accounting of disclosures as necessary to satisfy the Covered Entities obligations under 45 CFR 164.528. The Business Associate agrees to provide such information and/or documentation to the Covered Entity within thirty (30) days of a request for an accounting of disclosures. Business Associates agrees to forward all requests made directly to the Business Associate from individuals seeking an accounting of PHI.

9. **Confidential Communications**. Business Associate shall comply with any request from an individual to receive PHI via alternative means or at an alternative location approved by Covered Entity pursuant to 45 CFR 164.522(b), provided that Covered Entity notifies Business Associate in writing of the request

10. **Restrictions.** Business Associate shall comply with any restriction on the use or disclosure of protected health information that Covered Entity has agree to or is required to abide by under 45 CFR 164.522(a) provided that Covered Entity notifies Business Associate in writing of the restriction obligation.

11. **Minimum Retention**. Business Associate will retain the documentation required pursuant to §164.316(b)(1) for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

12. **Inspect.** The Business Associate agrees that from time to time, upon reasonable notice, it shall allow the Covered Entity or its authorized agents or contractors, to inspect or review the facilities, systems, books, records and procedures of the Business Associate to monitor compliance with this Agreement or any other state or federal security safeguard review. In the event the Covered Entity, in its sole discretion, determines that the Business Associate has violated any term of this Agreement, the Privacy Rule or Security Rule, it shall so notify the Business Associate in writing. The Business Associate shall promptly remedy the violation of any term of this Agreement and shall certify same in writing to the Covered Entity. The fact that the Covered Entity or its authorized agents or contractors inspect, fail to inspect or have the right to inspect the Business Associate's facilities, systems, books, records, and procedures does not relieve the Business Associate of its responsibility to comply with this Agreement. The Covered Entity's (1) failure to detect, or (2) detection but failure to notify the Business Associate, or (3) failure to require the Business Associate to remediate any unsatisfactory practices, shall not constitute acceptance of such practice or a waiver of the Covered Entity's enforcement rights under this Agreement. Nothing in this paragraph is deemed to waive Section G of this Agreement or the New Jersey Tort Claims Act, NJSA 59:1-1 et seq., as they apply to the Covered Entity

13. **Cooperation**. The Business Associate shall make itself, and any employees, subcontractors or agents assisting the Business Associate in the performance of its obligations under this Agreement and the Underlying Agreement, available to testify as witnesses or otherwise, in the event of litigation or administrative proceedings being commenced against the Covered Entity, its officers, employees, based upon a claimed violation of the Privacy Rule, the Security Rule or other law relating to security and privacy, except where the Business Associate or its employee, subcontractor or agent is a named adverse party.

14. **Response to Subpoena**. In the event Business Associate receives a subpoena or similar notice or request from any judicial, administrative or other party which would require the production of PHI received from, or created for, Covered Entity, Business Associate shall promptly forward a copy of such subpoena, notice or request to Covered Entity to afford Covered Entity the opportunity to timely respond to the demand for its PHI as Covered Entity determines appropriate according to its state and federal obligations.

15. **Other Obligations.** To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the Privacy Rule and/or Security Rule, the Business Associate shall comply with the requirements of such rules that apply to the Covered Entity in performance of such obligation(s).

C. <u>Permitted Uses and Disclosures</u>

16. **General Uses.** The Business Associate shall not use or disclose PHI other than as permitted or required by the Agreement or as required by law. The Business Associate may use PHI for the functions, activities, or services performed for or on behalf of the

Covered Entity as specified in the Contract provided that such use or disclosure would not violate this Agreement, the HIPAA regulations, or the HITECH Act. In the event that this Agreement conflicts with any other written agreement made between the Parties relating to the exchange of PHI, this Agreement shall control.

17. **General Disclosures.** The Business Associate may disclose PHI for proper business management and administration of the Business Associate or to carry out its legal responsibilities provided that such disclosure is required by law, or the disclosure would not violate this Agreement, the Privacy Rule, or Notice of Privacy Practices if done by the Covered Entity, the Business Associate executes a business associate agreement containing the same restrictions and conditions that apply through this Agreement to the Business Associate with respect to such PHI with a subcontractor/person receiving the PHI, and the subcontractor/person notifies the Business Associate of any instances of which it is aware that the confidentiality of PHI has been breached. In the event that this Agreement conflicts with any other agreement relating to the access or use or disclosure of PHI, this Agreement shall control.

18. **Use and Disclosure with Subcontractor.** A Business Associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain and transit protected health information on its behalf provided the Business Associate obtains satisfactory assurances in accordance with 45 CFR 164.504.(e)(5). Use and disclosure is limited to the permitted use and disclosures of this agreement or contract.

19. **Minimum Necessary.** Business Associate agrees to limit any use, disclosure, or request for use or disclosure of Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of the Privacy Rule.

D. Obligations of Covered Entity

20. **Notice of Privacy Practice**. In accordance with 45 CFR 164.520, the Covered Entity shall notify the Business Associate of any limitations in the Covered Entity's Notice of Privacy Practices to the extent that such limitation may affect the Business Associate's use or disclosure of PHI.

21. **Notification of Permissions.** The Covered Entity shall notify the Business Associate of any changes in or revocation of permission by an individual to use or disclose PHI, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

22. **Notification of Restrictions.** The Covered Entity shall notify the Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

23. **Impermissible Requests by Covered Entity.** The Covered Entity shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity or under the Covered Entity's Notice of Privacy Practices or other policies adopted by the Covered Entity pursuant to the Privacy Rule.

E. Term and Termination

24. **Term**. This Agreement shall be effective as of the date the Agreement is fully executed shall remain in effect until all PHI is returned to Covered Entity or destroyed in accordance with the terms of this Agreement.

25. **Return or Destruction of PHI**. Return PHI, and any Related Data, to Covered Entity in whatever form or medium that Business Associate received from or created on behalf of Covered Entity. In such case, no copies of such PHI and Related Data shall be retained. PHI and Related Data shall be returned as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of this Agreement or the underlying Agreement. Business Associate may destroy PHI and any Related Data provided that Covered Entity has agreed. All PHI and related data must be destroyed using technology or a methodology that renders the PHI, or Related Data, unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in its guidance http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html. Acceptable methods for destroying PHI or Related Data include: (A) paper, film, or other hard copy media shredded or destroyed in order that PHI or Related Data cannot be read or reconstructed; and (B) electronic media cleared, purged or destroyed consistent with the standards of the National Institute of Standards and Technology (NIST). Redaction as a method of destruction of PHI or Related Data is specifically excluded. This provision shall also apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of PHI

26. **Infeasible Return or Disposal of PHI**. In the event that the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction infeasible. The Covered Entity shall have the discretion to determine whether it is feasible for the Business Associate to return or destroy the PHI. If the Covered Entity determines it is feasible, the Covered Entity shall specify the terms and conditions for the return or destruction of PHI at the expense of the Business Associate. Upon the Covered Entity determining that the Business Associate cannot return or destroy PHI, the rights and obligations of the Parties established under this Agreement, HIPAA and the underlying regulations in regard to PHI shall survive the termination of this Agreement and shall continue, and the Business Associate shall limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI.

27. Certification. Except when determined that the PHI cannot be returned or destroyed, the Business Associate shall provide the Covered Entity with a certification, within thirty (30) days of termination of the Agreement, that neither it nor its subcontractors or agents maintains any PHI received, maintained, created, used or transmitted by the Business Associate on behalf of the Covered Entity under this Agreement, in any form, whether paper, electronic, film or other. The Covered Entity shall acknowledge receipt of such certification and, as of the date of such acknowledgement, this Agreement shall terminate.

F. Breach Obligations

28. Effects of a Material Breach of this Agreement. Upon the Covered Entity's knowledge of a material breach or violation(s) of any of the obligations under this Agreement by the Business Associate, the Covered Entity shall, at its discretion, either:

a. Provide an opportunity for the Business Associate to cure the breach or

b. End the violation, upon such terms and conditions as the Covered Entity has specified, the Covered Entity may terminate this Agreement and require that the Business Associate fully comply with the procedures specified in Section E., "Term and Termination."

G. Indemnification and Release

29. The Business Associate shall assume all risk and responsibility for, and agrees to indemnify, defend and save harmless the Covered Entity, its officers, agents and employees and each and every one of them, from and against any and all claims, demands, suits, actions, recoveries, judgments, costs (including attorneys' fees and costs and court costs), and expenses in connection therewith, on account of loss of life, property or injury or damages to the person, body or property of any person or persons, whatsoever, which shall arise from or result directly or indirectly from the Business Associate's use or misuse of PHI or from any action or inaction of the Business Associate or its officers, employees, agents or contractors with regard to PHI or the requirements of this Agreement, the Privacy Rule or Security Rule. Except in cases where indemnification is not permitted by law, this indemnification clause shall in no way limit the obligations assumed by the Business Associate under this Agreement, nor shall it be construed to relieve the Business Associate from any liability, nor preclude the Covered Entity from taking any other actions available to it under any other provisions of this Agreement, the Privacy Rule or at law.

30. Notwithstanding the above, the obligations assumed by the Business Associate herein shall not extend to or encompass suits, costs, claims, expenses, liabilities and judgments incurred solely as a result of actions or inactions of the Covered Entity.

31. The Business Associate further acknowledges the possibility of criminal sanctions and penalties for breach or violation of this Agreement or the Privacy Rule pursuant to 42 USC 1320d-6 and agrees to not seek indemnification from Covered Entity if such are imposed upon the Business Associate.

32. The Business Associate shall be responsible for, and shall at its own expense, defend itself against any and all suits, claims, losses, demands or damages of whatever kind or nature, arising out of or in connection with an act or omission of the Business Associate, its employees, agencies, or contractors, in the performance of the obligations assumed by the Business Associate pursuant to this Agreement. The Business Associate hereby releases the Covered Entity from any and all liabilities, claims, losses, costs, expenses and demands of any kind or nature whatsoever, arising under State or federal laws, out of or in connection with the Business Associate's performance of the obligations assumed by the Business Associate pursuant to this Agreement.

33. The obligations of the Business Associate under this section shall survive the expiration of this Agreement.

H. Miscellaneous

34. Data Ownership. Neither the Business Associate nor its agents or subcontractors shall hold any data ownership rights with respect to the Protected Health Information created, used, maintained, or transmitted by the Business Associate for the Covered Entity under this Agreement.

35. Governing Law. Except where federal law applies, this Agreement shall be governed by, construed and enforced in accordance with the laws of the State of New Jersey without regard to principles of conflict of laws.

36. Regulatory Reference. A reference in this Agreement to a section in the Privacy Standards, Security Standards, HIPAA or 42 C.F.R. Part 2 means the section as in effect or as amended.

37. Severability. The invalidity or unenforceability of any term or provision of this Agreement shall not affect the validity or enforceability of any other term or provision.

38. Amending Agreement. The Business Associate and the Covered Entity agree to take such action as is necessary to amend this Agreement from time to time in order that the Covered Entity can continue to comply with the requirements of the Privacy and Security Rules and case law that interprets the Privacy and Security Rules. All such amendments shall be in writing and signed by both Parties. The Business Associate and the Covered Entity agree that this Agreement may be superseded by a revised Business Associate Agreement executed between the Parties after the effective date of this Agreement.

39. Survival. The respective rights and obligations of the Business Associate and the Covered Entity under Section E, "Term and Termination" shall survive the termination of

the Contract. The respective rights and obligations of the Business Associate and the Covered Entity under Section G, "Indemnification and Release", shall survive the termination of this Agreement.

40. **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit the Covered Entity to comply with the HIPAA and the HIPAA regulations, as they may be amended or interpreted by a court of competent jurisdiction.

41. **Disclaimer**. The Covered Entity makes no warranty or representation that compliance by the Business Associate with this Agreement, HIPAA and the HIPAA regulations will be adequate or satisfactory for the Business Associate's own purposes. The Business Associate is solely responsible for all decisions made by the Business Associate regarding the safeguarding of PHI.

42. **Third Party Beneficiaries**. Nothing expressed or implied in the Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Business Associate and the Covered Entity, and any successor State agency to the Covered Entity, any rights, remedies, obligations or liabilities whatsoever.

43. **Individually Identifiable Information**. The Business Associate acknowledges that Social Security numbers and Social Security Administration (SSA) records, information or data regarding individuals (records) are confidential and require safeguarding. Failure to safeguard Social Security numbers and other SSA records can subject the Business Associate and its employees to civil and criminal sanctions under Federal and State laws including the Federal Privacy Act at 5 U.S.C. 552a; Social Security Act sections 205 and 1106 (see 42 U.S.C. 405(c)(2)(C)(viii) and 42 U.S.C. 1306, respectively); and N.J.S.A. 56:8-164. The Business Associate shall ensure that all persons who will handle or have access under this Agreement to any Social Security Number or other SSA record will be advised of the confidentiality of the records; the safeguarding requirements to protect the records and prevent unauthorized access, handling, duplication and re-disclosure of the SSA records; and the civil and criminal sanctions for failure to safeguard the SSA records. The Business Associate shall enact and/or maintain safeguards necessary to protect these records and prevent the unauthorized or inadvertent access to, duplication of or disclosure of a Social Security number or other SSA record.

44. **Medicaid Information**. The Business Associate acknowledges that all information related to the Children's Health Insurance Program (CHIP) and the Medicaid program is confidential, disclosure must be restricted to purposes directly connected with the administration of the CHIP and Medicaid State Plans, and Business Associate must comply with 42 C.F.R. 431.300 et seq. and N.J.A.C. 10:49-9.7. See also 42 U.S.C. 1396a(a)(7) and N.J.S.A. 30:4D-7.g. The Business Associate shall ensure that all persons who will handle or have access under this Agreement to Medicaid or CHIP information will be advised of the confidentiality of the records and the safeguarding requirements.

45. **Drug and Substance Abuse Records**. The Business Associate acknowledges that any record that directly or indirectly identifies an individual as a current or former patient of a drug or alcohol program, as those terms are defined at 42 CFR §2.11 is confidential. Confidentiality applies to such records of deceased patients. The Business Associate shall ensure that all persons who will handle or have access under this Agreement to drug or substance abuse information will be advised of the confidentiality of the records, requirements to protect the records and prevent unauthorized access, handling, duplication and re-disclosure, except as permitted under 42 CFR Part 2.

46. **Notice Requirements.** Any notices to be given hereunder shall be made via email and telephone, followed by notice via regular and certified U.S. mail, return receipt requested:

Business Associate: _____
_____
_____
_____
_____
_____

Covered Entity:

NJDOH Data Privacy Officer
New Jersey Department of Health
225 East State Street
PO Box 360
Trenton, NJ 08625
privacy.officer@doh.nj.gov
Phone: 609-292-5443

NJDOH Information Security Officer
c/o: Office of Information Technology Services
New Jersey Department of Health
P.O. Box 360
Trenton, NJ 08625
iso@doh.nj.gov
NJDOH OITS Help Desk (609) 984-0224

As the Covered Entity is a body corporate and politic of the State of New Jersey, the signature of its authorized representative is affixed below. The undersigned representative of the Covered Entity certifies that he or she is fully authorized to enter into the terms and conditions of this Agreement and to execute and legally bind the Covered Entity to this document.

Additionally, the undersigned representative of the Business Associate certifies that he or she is fully authorized to enter into the terms and conditions of this Agreement and to execute and legally bind the Business Associate to this document.

Covered Entity:	Business Associate:
_____	_____
Signature	Signature
[Name]	Printed Name: _____
[Title]	Title: _____
[Agency]	Agency: _____
Dated: _____	Dated: _____