BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT ("**Agreement**") is entered into by and between Tabula Rasa HealthCare Group, Inc. located at 228 Strawbridge Drive, Moorestown, NJ 08057 ("**Business Associate**"), and you ("**Covered Entity**").

RECITALS

WHEREAS, Business Associate has entered into that certain business agreement ("**Covered Entity Agreement**") pursuant to which Business Associate provides products and services to Covered Entity and in furtherance of such agreement Business Associate may from time to time perform on behalf of Covered Entity a function or activity supporting the Covered Entity that involves the Use or Disclosure of Protected Health Information ("**PHI**").

WHEREAS, Business Associate and Covered Entity desire to enter into this Agreement regarding the Use and/or Disclosure of PHI as required by the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), the Standards for Privacy of Individually Identifiable Health Information (the "**Privacy Rule**") and the Standards for Security of Electronic Protected Health Information (the "**Security Rule**") promulgated thereunder, and the Health Information Technology for Economic and Clinical Health Act (Division A, Title XIII and Division B, Title IV, of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5) (the "**HITECH Act**"), and the regulations implementing the HITECH Act.

NOW, THEREFORE, in consideration of the mutual promises below and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

AGREEMENT

A. General Compliance with HIPAA Privacy Rule and Security Rule.

The parties shall conduct their respective businesses in accordance with all applicable laws and regulations regarding the privacy and security of PHI, including, without limitation, HIPAA and the HITECH Act, as amended from time to time, and the regulations promulgated thereunder.

B. Definitions.

Terms used but not otherwise defined in this Agreement shall have the same meaning given to such terms in HIPAA, the HITECH Act, or any implementing regulations promulgated thereunder, including, but not limited to, the Privacy Rule and the Security Rule. In the event of a conflict regarding any definition in this Agreement and the

definitions in HIPAA, the HITECH Act, or any implementing regulations promulgated thereunder, including but not limited to the Privacy Rule and the Security Rule, the definitions in HIPAA, the HITECH ACT and any implementing regulations shall govern.

1. "**Breach**" means the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of PHI (within the meaning of 45 C.F.R. § 164.402).

2. "**Data Aggregation**" means, with respect to PHI created or received by Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

3. "**Designated Record Set"** means a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about Individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about Individuals. For the purposes of this paragraph, the term "**record**" means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a covered entity.

4. "**Disclose**" or "**Disclosure**" means the release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.

5. "**Electronic Protected Health Information"** or "**ePHI**" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

6. "**Individual**" means the person who is the subject of PHI and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

7. "**Individually Identifiable Health Information**" is information that is a subset of health information, including demographic information collected from an Individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and (i) that identifies the Individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

8. "**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

9. "**Protected Health Information**" or "**PHI**" means Individually Identifiable Health Information that is: (i) transmitted by "electronic media," as defined in 45 C.F.R. § 160.103; (ii) maintained in any medium described in the definition of electronic media; or (iii) transmitted or maintained in any other form or medium.

10. "**Required by Law**" means a mandate contained in law that compels an entity to make a Use or Disclosure of PHI and that is enforceable in a court of law.

11. "**Secretary**" means the Secretary of Health and Human Services or any other officer or employee of the U.S. Department of Health and Human Services to whom the authority involved has been delegated.

12. "**Security Incident**" means the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

13. "**Security Rule**" means the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164 Subpart C.

14. "**Unsecured Protected Health Information"** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

15. "**Use**" means the sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information.

C. Obligations and Activities of Business Associate.

1. Nondisclosure. Business Associate shall not Use or Disclose PHI other than as permitted or required by the Covered Entity Agreement, this Agreement or as Required by Law.

2. Minimum Necessary. Business Associate shall limit any PHI Used, Disclosed or requested to the minimum necessary to accomplish the intended purpose of the Use, Disclosure or request.

3. Safeguards. Business Associate shall use appropriate safeguards to prevent the Use or Disclosure of PHI other than as provided for by the Covered Entity Agreement or this Agreement.

4. Security Rule. Business Associate shall comply with the Security Rule provisions set forth in 45 C.F.R. Part 164, Subpart C, including the provisions relating to Security Standards General Rules (45 C.F.R. § 164.306), Administrative Safeguards (45 C.F.R. § 164.308), Physical Safeguards (45 C.F.R. § 164.310), Technical Safeguards (45 C.F.R. § 164.312), Organizational Requirements (45 C.F.R. § 164.314) and Policies and

Documentation (45 C.F.R. § 164.316), and to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

5. Reporting of Disclosures. Business Associate shall report, in writing, to Covered Entity any Use or Disclosure of PHI not provided for by the Covered Entity Agreement or Agreement of which Business Associate becomes aware.

6. Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

7. Business Associate's Agents. Business Associate shall ensure that any agents, including subcontractors, which create, receive, maintain or transmit PHI on behalf of Business Associate agree in writing to restrictions and conditions that are no less restrictive than those that apply to Business Associate through this Agreement with respect to PHI.

8. Access to PHI. At the written request of Covered Entity (and in the reasonable time and manner designated by Covered Entity), Business Associate shall provide access to PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity in writing, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524. This provision shall only apply if Business Associate has PHI in a Designated Record Set. Business Associate further shall notify Covered Entity of any requests for access it receives from an Individual within five (5) business days of receipt.

9. Documentation of Disclosures. Business Associate shall document such Disclosures of PHI and information related to such Disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528.

10. Accounting of Disclosures. At the written request of Covered Entity (and in the reasonable time and manner designated by Covered Entity), Business Associate shall provide to Covered Entity information collected in accordance with Section C.9 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528 (and HITECH Act § 13405(c). Business Associate further shall notify Covered Entity of any requests for accounting of Disclosures it receives from an Individual within ten (10) business days of receipt.

11. Amendment of PHI. At the written request of Covered Entity (and in the reasonable time and manner designated by Covered Entity) Business Associate shall make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs pursuant to 45 C.F.R. § 164.526. This provision shall only apply if Business Associate has PHI in

a Designated Record Set. Business Associate further shall notify Covered of any requests for amendment it receives from an Individual within fifteen (15) business days of receipt.

12. Internal Practices. Business Associate shall make its internal practices, books and records, including policies and procedures, relating to the Use and Disclosure of PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity, or to the Secretary, for purposes of determining Covered Entity's and/or Business Associate's compliance with the Privacy Rule and/or Security Rule.

13. Reporting of Potential Breaches and Security Incidents. Business Associate shall report in writing to Covered Entity any Security Incident or potential Breach of Unsecured Protected Health Information as follows:

a) Business Associate shall report any actual, successful Security Incident within two (2) days of Business Associate's discovery of such actual, successful Security Incident.

b) Business Associate shall report any attempted, unsuccessful Security Incident of which Business Associate becomes aware at the written request of Covered Entity but in no event more frequently than on a quarterly basis.

c) Business Associate shall report any potential Breach of Unsecured Protected Health Information within two (2) days of discovery.

In each instance (a) through (c) above, the written report shall include the following: (i) the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired, Used or Disclosed during any such Security Incident or potential Breach, to the extent known by Business Associate; (ii) such other information regarding the Security Incident or potential Breach as is known to Business Associate at the time the report is made (such as the type of PHI involved, the nature of the information accessed, acquired, Used or Disclosed, etc.); and (iii) an acknowledgement by Business Associate that the information provided pursuant to (i) and (ii) shall be supplemented if and when further information becomes available to Business Associate.

14. Additional Responsibility. To the extent Business Associate is to carry out an obligation of Covered Entity under the Privacy Rule provisions set forth at 45 C.F.R. Part 164, Subpart E, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation. Business Associate shall comply with the obligations set forth in Exhibit 1 "Physical Security, Privacy and Safety Requirements" which is attached hereto and incorporated herein by reference.

D. Permitted Uses and Disclosures by Business Associate.

1. Permitted Uses and Disclosures. Except as otherwise limited in this Agreement, Business Associate may Use or Disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Covered Entity Agreement, provided such Use or Disclosure would not violate the Privacy Rule if done by Covered Entity.

2. Use for Management and Administration. Except as otherwise limited in this Agreement, Business Associate may Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

3. Disclosure for Management and Administration. Except as otherwise limited in the Covered Entity Agreement and this Agreement, Business Associate may Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that: (a) the Disclosures are Required by Law, or (b) Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will remain confidential and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and (c) the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Data Aggregation. Except as otherwise limited in this Agreement, Business Associate may Use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

5. De-identified Data. Business Associate may de-identify PHI in accordance with the standards set forth in 45 C.F.R. § 164.514(b) and may use or disclose such de-identified data unless prohibited by applicable law.

E. Obligations of Covered Entity.

1. Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices from Covered Entity, as well as any limitations and/or changes to such notice, of which Covered Entity is notified, to the extent that such limitations and/or changes may affect Business Associate's Use or Disclosure of PHI.

2. Changes in Permission. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to Use or Disclose PHI, of which Covered Entity is notified, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI.

3. Notification of Restrictions. Covered Entity shall 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 and of which Covered Entity is notified, to the extent that such restriction may affect Business Associate's Use or Disclosure of PHI.

4. Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate Use or Disclose PHI in any manner that would not be permissible under HIPAA, as amended by the HITECH Act, or any implementing regulations.

F. Term and Termination.

1. Term. The term of this Agreement shall be effective as of the date of the Covered Entity Agreement and shall terminate upon the earlier of: (i) the date of termination of the Covered Entity Agreement, or (ii) the date upon which Business Associate no longer provides functions or services subject to this Agreement for, or on behalf of, Covered Entity.

2. Termination for Cause. Notwithstanding any other provision of this Agreement to the contrary, (i) either party may terminate the Covered Entity Agreement and/or this Agreement in the event of a material breach of any term of this Agreement by the other party which is not corrected within thirty (30) days of receipt of written notice describing the nature of the alleged breach, and (ii) Covered Entity may immediately terminate the Covered Entity Agreement and/or this Agreement in the event of a material breach of this Agreement that involves a Breach of Unsecured PHI.

3. Effect of Termination. Except as provided in this Section F.3, upon termination of this Agreement for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of Business Associate or subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI. In the event that Business Associate believes that returning or destroying PHI is not feasible, Business Associate shall notify Covered Entity in writing of the conditions that make return or destruction infeasible. Upon mutual agreement of Covered Entity and Business Associate that return or destruction of the PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

4. Indemnification. Business Associate agrees to indemnify and hold harmless Covered Entity and its affiliates and their respective current and former officers, directors, members, employees and agents (collectively, "**Indemnitees**"), from and against any liability, claim, action, loss, cost, damage or expense (including reasonable fees of attorneys and experts) incurred or suffered by Indemnitees, to the extent that such liability, claim, action, loss, cost, damage, expense or fees are attributable to or incurred as a result of an unauthorized Use or Disclosure of PHI by Business Associate or its subcontractor or agent; an acquisition, access, Use, or Disclosure, by Business Associate or its subcontractor or agent, that constitutes a Breach or Security Incident; any breach of this Agreement by Business Associate; or any breach of the agreement described in Section C.7 of this Agreement by Business Associate's subcontractor or agent.

G. Miscellaneous.

1. Regulatory References. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended, and for which compliance is required.

2. Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time for Covered Entity and Business Associate to comply with the requirements of the Privacy Rule and Security Rule, HIPAA, the HITECH Act and its implementing regulations that are binding on such party.

3. Survival. The respective rights and obligations of Business Associate under Sections F.3 and F.4 of this Agreement shall survive the termination of this Agreement.

4. Interpretation. The parties agree that any ambiguity in this Agreement or conflict with the terms of the Covered Entity Agreement shall be resolved to permit the parties to comply with HIPAA and the HITECH Act and any implementing regulations promulgated thereunder, including but not limited to the Privacy Rule and Security Rule and applicable state laws.

5. No Third-Party Beneficiary. Notwithstanding any other provision of this Agreement to the contrary, if any, nothing in this Agreement, or in the parties' course of dealings, shall be construed as conferring any third-party beneficiary status with respect to this Agreement on any person not a party to this Agreement.

6. Assignment. This Agreement may not be transferred or assigned by either party without the prior written consent of the other party.

7. Governing Law. All questions with respect to the construction of this Agreement and the rights and liabilities of the parties except as otherwise provided, shall be determined in accordance with the laws of New Jersey without regard to conflicts of laws principles. All disputes hereunder shall be resolved in the applicable state or federal courts in the State of New Jersey. The parties consent to the jurisdiction of such courts and waive any jurisdictional or venue defenses otherwise available.

8. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original but all of which shall constitute one and the same instrument.

9. Effect of Agreement. This Agreement sets forth the entire agreement and understanding between the parties regarding the subject matter hereof and supersedes all other discussions, representations, agreements and understandings of every kind, whether oral or written, with respect to the subject matter hereof. In the event of a conflict between the terms of this Agreement and the terms of the Covered Entity Agreement or any agreement for services between the parties, the terms of this Agreement shall control.

(Remainder of page left blank intentionally)

EXHIBIT 1

PHYSICAL SECURITY, PRIVACY AND SAFETY REQUIREMENTS

Business Associate agrees to the following security and privacy safeguards. Additionally, Business Associate agrees to comply with all security requirements for upstream contracted entities. Covered Entity will provide any security requirements in writing.

1. Business Associate will implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. § 164.310(a)(1)

2. Business Associate will establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. § 164.310(a)(2)(i)

3. Business Associate will implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. § 164.310(a)(2)(ii)

4. Business Associate agrees to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, control of access to software programs for testing and revision, and creation of audit trails including visitor and personnel access logging history. § 164.310(a)(2)(iii)

5. Business Associate will implement policies and procedures to ensure that physical and logical access is removed for any of its personnel that are reassigned from the Covered Entity's account/functions, suspended and/or terminated.

6. Business Associate will implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks). § 164.310(a)(2)(iv)

7. Business Associate will implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. § 164.310(b)

8. Business Associate will implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. § 164.310(c)

9. Business Associate will implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health

information, into and out of a facility, and the movement of these items within the facility. § 164.310(d)(1)

10. Business Associate will maintain a record of the movements of hardware and electronic and any person responsible therefore. § 164.310(d)(2)(iii)

11. Business Associate will implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. § 164.310(d)(2)(i)

12. Business Associate data/information shall be returned to Covered Entity or destroyed via secure and commercially reasonable processes when use is no longer needed.

13. Business Associate will implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. § 164.310(d)(2)(ii)

14. Business Associate will create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. § 164.310(d)(2)(iv)

15. Covered Entity's data/information shall not be stored at Business Associate's facilities or those of its contractors unless it is required. If storage of Covered Entity's data/information storage is required in the performance of this agreement then it must be stored encrypted, within a physically secured environment.

16. Business Associate shall promptly notify Covered Entity security or compliance staff of any on-site security, privacy or safety incident, threat and/or emergency that threatens, interrupts or threatens to interrupt Covered Entity related processes, information or interests. Business Associate shall have an incident response plan and include notifications to Covered Entity for incidents, issues or threats that impact or have a reasonable chance to impact Covered Entity.

17. Business Associate personnel shall reasonably cooperate with any audit, inquiry, security response or investigation in response to any security, privacy or safety incident, threat and/or emergency related to Covered Entity.

18. Business Associate will implement policies and procedures to comply with the HIPAA Privacy Rule, 45 CFR parts 160 and 164, along with the general precepts of individual privacy, data security, availability and integrity of Individually Identifiable Health Information as part of this agreement.

19. Business Associate shall ensure that all of its products and services provided to Covered Entity under this agreement shall be provided in compliance with all federal and state laws and regulations governing the privacy and security of Protected Health Information.

20. Business Associate agrees not to use or disclose Protected Health Information other than as permitted under this Business Associate Agreement or otherwise required by law.

21. Business Associate will implement policies and procedures which include appropriate consequences or disciplinary action against any member of their workforce who violates the privacy obligations of this agreement.

22. Business Associate agrees to submit to an initial on-site security review and subsequent periodic security reviews for all Covered Entity site locations, whether controlled directly by the Business Associate or indirectly using subcontractors, where Covered Entity information and/or assets are stored or processed.

23. Business Associate agrees to complete a background check for all personnel completing services for Covered Entity. Business Associate agrees to exclude any person that has been identified of having any felony conviction(s) or having a misdemeanor conviction(s) related to theft, fraud or healthcare related crimes (including but not limited to, shoplifting, larceny, embezzlement, forgery, credit card fraud or check fraud), and/or appearing on any exclusion or sanction lists relating to federal or state healthcare programs, such as but not limited to OIG, LEIE, GSA SAM, State Medicare and Medicare list will automatically exclude an individual from employment.

24. Business Associate is to promptly notify Covered Entity if it learns that any of its personnel, contractors or subcontractor personnel assigned to work with Covered Entity information or assets are believed to be involved in criminal conduct and/or are the subject of formal criminal charges or criminal convictions.

(Remainder of page left blank intentionally)