BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is effective as of _____, _____ ("Effective Date") and is by and between The Washington University, a benevolent corporation created by special act of the Missouri General Assembly, on behalf of itself and/or its affiliated organization(s) ("Covered Entity") and _____, a _____ _____ ("Business Associate").

RECITALS

A. Covered Entity and Business Associate are parties to an agreement or arrangement pursuant to which Business Associate performs certain services (the "Services") for Covered Entity.

B. Covered Entity may Disclose or make available to Business Associate, and Business Associate may Use, Disclose, receive, transmit, maintain or create from or on behalf of Covered Entity, health information that is considered PHI (as defined below) in connection with the provision of Services to or on behalf of Covered Entity.

C. The parties are committed to compliance with the Health Insurance Portability and Accountability Act of 1996 and regulations promulgated thereunder, as amended from time to time (collectively, "HIPAA").

D. The purpose of this Agreement is to satisfy the obligations of Covered Entity and Business Associate under HIPAA and ensure the integrity and confidentiality of PHI that Business Associate Uses, Discloses, receives, transmits, maintains or creates from or on behalf of Covered Entity.

AGREEMENT:

NOW, THEREFORE, in consideration of the foregoing recitals and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions. Capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164, the HITECH Standards or any future regulations promulgated or guidance issued by the Secretary thereunder.

A. "Breach" shall have the same meaning as that term is defined and used in the Breach Notification Rule.

B. "Breach Notification Rule" shall mean the provisions of 45 CFR Parts 160 and 164, Subpart D, entitled Breach Notification for Unsecured Protected Health Information Rules.

C. "Discover" or "Discovery" shall mean, with respect to a Use or Disclosure by Business Associate not provided for by this Agreement including, without limitation, any Breach, the earlier to occur of: (1) Business Associate's actual knowledge of such Use or Disclosure; (2) the first day on which Business Associate, by exercising reasonable diligence, reasonably would have known of such Use or Disclosure; or (3) the first day on which such Use or Disclosure reasonably would have been known, by exercising reasonable diligence, to any person, other than the person committing the Use or Disclosure, who is an employee, officer or other agent of the Business Associate.

D. "Electronic Protected Health Information" or "ePHI" shall have the same meaning as the term "electronic PHI" in the Security Rule, to the extent information is created, maintained, or received by, or transmitted to or by, Business Associate to, from or on behalf of Covered Entity.

E. "HITECH" means Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§17921-17954 and its implementing regulations, when and as each is effective.

F. "Individual" shall have the same meaning as the term "individual" in the Privacy Rule, and shall include a person who qualifies as a personal representative in accordance with the Privacy Rule.

G. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, subparts A and E, as amended from time to time.

H. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in the Privacy Rule, to the extent such information is created, maintained, or received by, or transmitted to or by, Business Associate to, from or on behalf of Covered Entity.

I. "Required By Law" shall have the same meaning as the term "required by law" as used in the Privacy Rule.

J. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

K. "Security Incident" shall have the same meaning as the term "security incident" in the Security Rule.

L. "Security Rule" shall mean the Security Standards for the Protection of Electronic PHI at 45 C.F.R. Parts 160 and 164, Subparts A and C, as amended from time to time.

2. Scope. This Agreement applies to and shall be, and hereby is, automatically incorporated into all present and future agreements and relationships, whether written, oral or implied, between Covered Entity and Business Associate, pursuant to which PHI is created, maintained, or received by, or transmitted to or by, Business Associate to, from or on behalf of Covered Entity in any form or medium whatsoever. As of the effective date of this Agreement, this Agreement automatically extends to, is incorporated into and amends all existing agreements between Covered Entity and Business Associate involving the Use or Disclosure of PHI.

3. Purpose; General Rules. This Agreement sets forth the terms and conditions pursuant to which Business Associate shall handle all PHI that is used, disclosed, received, transmitted, maintained, or created by Business Associate from, to or on behalf of Covered Entity and subcontract any portion of the services it provides to Covered Entity. All Uses and Disclosures of PHI by Business Associate not Required by Law, authorized by this Agreement, or authorized by any other written agreement with Covered Entity or Covered Entity's written instructions are prohibited.

4. Relationship of Parties. In the performance of the work, duties and obligations described in this Agreement or in any other agreement between the parties, the parties acknowledge and agree that each party is at all times acting and performing as an independent contractor and at no time shall the relationship between the parties be construed as a partnership, joint venture, employment, principal/agent relationship, or master/servant relationship.

5. Ownership of PHI. Business Associate acknowledges that all right, title and interest in and to any information, including without limitation PHI, furnished to Business Associate vests solely and exclusively with Covered Entity or the Individual to whom such PHI relates.

6. Permitted Activities of Business Associate. Except as otherwise limited in this Agreement, Business Associate may:

A. **Use** PHI for the proper management and administration of Business Associate, to carry out the legal responsibilities of Business Associate, provided such Uses are permitted under applicable federal and state confidentiality laws.

B. **Use or Disclose** PHI to perform services for Covered Entity provided that such use or disclosure would not violate HIPAA if done by Covered Entity.

C. **Disclose** PHI in its possession for its proper management and administration or to carry out its legal responsibilities, provided such disclosures are permitted under applicable federal and state confidentiality laws and are: (i) Required by Law, or (ii) Business Associate obtains reasonable assurances from the third party to whom the information is disclosed that such PHI will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the third party, and the third party notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

7. <u>Protection of PHI by Business Associate</u>. Business Associate shall:

A. Not use or disclose PHI other than as permitted or required by this Agreement, any underlying agreement between the parties, or as Required By Law.

B. Make reasonable efforts to limit requests for and the use and disclosure of PHI to a Limited Data Set (as defined in 45 C.F.R. § 164.514(e)(2)) or to the Minimum Necessary PHI (as defined in 45 C.F.R. § 164.514(d)) to accomplish the intended purpose of such use, disclosure or request.

C. Use appropriate, commercially reasonable safeguards to prevent the use or disclosure of PHI other than those uses or disclosures provided for by this Agreement and comply with the Security Rule with respect to ePHI.

D. Develop and implement administrative, physical and technical safeguards, at its expense, as may be required from time to time to maintain compliance with HIPAA and HITECH and to reasonably and appropriately protect the confidentiality, integrity and availability of ePHI that it creates, receives, maintains or transmits on behalf of Covered Entity and to prevent non-permitted or violating Uses or Disclosures of ePHI.

E. Mitigate, to the extent practicable, any harmful effect of an unauthorized use or disclosure of PHI by Business Associate, or a subcontractor, vendor, or agent of Business Associate, in violation of the requirements of this Agreement.

F. Report without unreasonable delay, and in no event later than three (3) business days, to the designated privacy officer of Covered Entity any Security Incident Business Associate Discovers.

G. Notify the designated privacy officer of Covered Entity after Business Associate's Discovery of a Breach without unreasonable delay, and in no event later than three (3) business days after Business Associate, or any of its employees or agents, Discovered the Breach. Such notification shall include, to the extent possible, the identification of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the Breach and any other information available to Business Associate about the Breach which is required to be included in the notification of the Breach provided to the Individual in accordance with 45 C.F.R. §164.404(c). Business Associate will notify Covered Entity prior to any communication with Individuals affected by any Breach. If Business Associate (or one of its subcontractors, vendors or agents) is responsible for a Breach, Covered Entity may, at its option, require Business Associate to provide any of the notifications required by 45 C.F.R. § 164.404 at Business Associate's expense, the content of which shall be created by Covered Entity.

H. Ensure that any agents, including subcontractors, to whom Business Associate provides PHI received from, or created or received by Business Associate on behalf of Covered Entity, agrees in writing to the same restrictions and conditions that apply to Business Associate with respect to such information, including requiring a subcontractor or agent to agree in writing to comply with the Security Rule with respect to any ePHI

provided to such subcontractor or agent, and monitor any such subcontractor for any pattern of activity that could constitute a material breach of such subcontractor's obligations and take reasonable steps to cure the breach, end the violation or terminate the subcontractor relationship.

I. Provide access, at the request of Covered Entity, to PHI in a Designated Record Set to Covered Entity or to an Individual or another person properly designated by the Individual, in order to meet the requirements under 45 C.F.R. § 164.524. If Business Associate maintains PHI electronically in a Designated Record Set and if the Individual requests an electronic copy of such information, Business Associate must provide Covered Entity, or the Individual or person properly designated by the Individual, as directed by Covered Entity, access to the PHI in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual. Any fee that Business Associate may charge for such electronic copy shall not be greater than Business Associate's labor and supply costs in responding to the request.

J. Make any amendment(s) to PHI in its possession contained in a Designated Record Set at the request of Covered Entity or an Individual pursuant to 45 C.F.R. § 164.526, in a time and manner to satisfy Covered Entity's obligations under 45 C.F.R. 164.526.

K. Document 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, including those made through an electronic health record in accordance with HITECH, in accordance with 45 C.F.R. § 164.528 and provide such information to Covered Entity within ten (10) business days of a written request from Covered Entity.

L. Make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI available to the Secretary for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule.

M. Comply with the requirements of the Privacy Rule, Security Rule and HITECH Act that apply to Covered Entity in the performance of Business Associate's delegated obligation.

N. Not sell PHI, as defined in 42 CFR §164.502(a)(5)(ii).

O. Not make any disclosure of PHI of an Individual who has requested to restrict disclosure of PHI where the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law, and the PHI pertains solely to a health care item or service for which the Individual or person other than the health plan on behalf of the Individual, has paid Covered Entity in full.

P. Provide evidence of a Service Organization Control (SOC) Type 2 audit report performed by an independent auditor within the last (2) years that verifies appropriate security controls and safeguards are in place to the extent Business Associate has access to at least 500 patient records for all Trust Services Principles.

8. <u>Obligations of Covered Entity</u>. Covered Entity shall:

A. Notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 C.F.R. 164.520, to the extent such limitation may affect Business Associate's use or disclosure of Protected Health Information.

B. Notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

C. Notify Business Associate of any restriction on the use or disclosure of Protected Health

Information that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522 to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

9. Indemnification, Settlement and Procedure. Business Associate shall indemnify, defend and hold harmless Covered Entity and any of Covered Entity's affiliates, and their respective officers, trustees, directors, employees and agents (an "Indemnitee") from and against any claim, cause of action, liability, damage, cost, fine, penalty or expense (including, without limitation, reasonable attorneys' fees and court costs) (collectively, "Loss") arising out of or in connection with any unauthorized or prohibited use or disclosure of PHI by Business Associate, any subcontractor or any agent or person under Business Associate's control, except to the extent such Loss is caused by Covered Entity's negligence or willful misconduct. In the event a claim is made against an Indemnitee for any such claim, cause of action, liability, damage, cost, penalty or expense, Business Associate shall provide qualified and competent counsel, reasonably acceptable to Indemnitee, to represent the Indemnitee's interest at Business Associate's expense. Covered Entity shall have the sole right to control and approve any settlement or other compromise of any claim brought against it that is covered by this Section.

10. Injunctive Relief; Acknowledgment. Business Associate acknowledges that the restrictions contained in this Agreement are reasonable and necessary to protect the legitimate professional and business interests of Covered Entity and to ensure Covered Entity's compliance with HIPAA. Business Associate further acknowledges and agrees that a breach of the covenants contained in this Agreement will cause irreparable harm to Covered Entity and that damages arising from any such breach may be difficult to ascertain and no adequate legal remedy exists. Accordingly, in such situation Covered Entity shall be entitled to receive injunctive relief and/or specific performance and damages, as well as any and all legal or equitable remedies to which it may be entitled.

11. Term and Termination

A. Term. The term of this Agreement shall commence on the Effective Date, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is not feasible to return or destroy the PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

B. Termination for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall either, at its sole discretion:

i. Provide an opportunity for Business Associate to cure the breach/end the violation, and terminate this Agreement if Business Associate does not cure the breach/end the violation within the time specified by Covered Entity; or

ii. Immediately terminate this Agreement.

Business Associate shall ensure that it maintains the termination rights in this Section in any agreement it enters into with a subcontractor.

C. Obligations of Business Associate upon Termination.

i. Except as provided in paragraph (ii) of this Section, upon termination of this Agreement, for any reason, Business Associate shall return to Covered Entity or, if agreed to by Covered Entity, destroy all PHI received from Covered Entity, or created, maintained or received by Business Associate on behalf of Covered Entity that the Business Associate maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

ii. Business Associate and its subcontractors and agents shall not retain copies of the PHI except to the extent necessary for the Business Associate to carry out its own management and administration or its legal responsibilities after termination of this Agreement provided that Business Associate shall extend the protections of this Agreement to such PHI.

12. Miscellaneous

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

B. Amendment. No change, amendment, or modification of this Agreement shall be valid unless set forth in writing and agreed to by both parties. Notwithstanding the foregoing, 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 required to ensure compliance with such developments ("Required Amendment"), and therefore this Agreement shall be deemed automatically amended to the extent necessary for Covered Entity to continue to comply with the requirements of HIPAA and its implementing regulations, including, without limitation, the Privacy Rule, the Security Rule and the Breach Notification Rule, as those requirements may be amended from time to time. Unless otherwise specified, any Required Amendment shall be effective when provided to Business Associate in writing ("Amendment Notice").

C. Survival. The provisions and respective rights and obligations of the parties under Sections 2, 5, 6, 7, 8, 9, 10, 11, and 12 of this Agreement shall survive the termination of this Agreement.

D. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity and Business Associate to comply with HIPAA.

E. Notice. Any notice, report or other communication required under this Agreement shall be in writing and shall be delivered personally, telegraphed, emailed, sent by facsimile transmission, or sent by U.S. mail.

F. Governing Law. The rights, duties and obligations of the parties to this Agreement and the validity, interpretation, performance and legal effect of this Agreement shall be governed and determined by applicable federal law with respect to HIPAA and otherwise by the laws of the state of Missouri.

G. No Third Party Beneficiaries. There are no intended third party beneficiaries to this Agreement. Without in anyway limiting the foregoing, it is the parties' specific intent that nothing contained in this Agreement give rise to any right or cause of action, contractual or otherwise, in or on behalf of any Individual whose PHI is used or disclosed pursuant to this Agreement.

H. Waiver. No provision of this Agreement shall be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

I. Authority. The persons signing below have the right and authority to execute this Agreement for their respective entities and no further approvals are necessary to create a binding Agreement.

J. Conflicts. In the event of any conflict between the terms and conditions stated within this Agreement and those contained within any other agreement or understanding between the parties (written, oral, or implied), the terms of this Agreement shall govern. Without limiting the foregoing, no provision of any other agreement or understanding between the parties limiting the liability of Business Associate to Covered Entity shall apply to the breach of any term, condition or covenant contained in this Agreement by Business Associate.

K. Headings. The headings of each section are inserted solely for purposes of convenience and shall not alter the meaning of this Agreement.

IN WITNESS THEREOF, each party has caused this Agreement to be executed by its duly authorized representative.

COVERED ENTITY: **WASHINGTON UNIVERSITY**	**BUSINESS ASSOCIATE:**
Authorized Signature	Authorized Signature
Title	Title
Date	Date