BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") is made and entered into as of _____, (the "Effective Date") by and between The Methodist Hospital d/b/a Houston Methodist Hospital and its subsidiary corporations which are covered entities under the HIPAA Laws, as defined below ("Covered Entity") and _____ ("Business Associate"), each a "Party" and collectively the "Parties".

WHEREAS, Business Associate and Covered Entity are parties to one or more service agreements pursuant to which Business Associate provides certain services to Covered Entity (the "Services Agreement"); and

WHEREAS, the services provided by Business Associate to Covered Entity cause it to be considered a "business associate" of Covered Entity under privacy and information security regulations, including the regulations contained in 45 C.F.R. Parts 160 and 164; and

WHEREAS, pursuant to the Services Agreement, Business Associate will have access to Protected Health Information ("PHI") (as defined below) of Covered Entity; and

WHEREAS, Covered Entity is required to obtain written satisfactory assurances from business associates who create, receive, maintain or transmit PHI on behalf of Covered Entity that such business associates will appropriately safeguard the PHI in accordance with the HIPAA Laws (as defined below); and

WHEREAS, Business Associate and Covered Entity desire to incorporate into the Services Agreement certain provisions required to be implemented by Business Associate under the HIPAA Laws.

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein, the sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. **Definitions**. For purposes of this Agreement, all capitalized terms used herein but not specifically defined herein will have the meanings given to them in the HIPAA Laws, the HITECH Act, and the regulations promulgated thereunder.

(a) "HIPAA Laws" means § 264 of the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, the Administrative Simplification Provisions of the Social Security Act, 42 U.S.C. §§ 1320d-1320d-8 and the regulations promulgated at 45 C.F.R. Parts 160 and 164, as amended by the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 17921-17954, as may be further amended from time to time.

(b) "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act included in the American Recovery and Reinvestment Act of 2009 and codified at 42 U.S.C. §17921-17954.

(c) "Protected Health Information" or "PHI" has the meaning set forth in the HIPAA Laws.

2. **Uses and Disclosures of PHI.**

(a) 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 reasonably necessary for Business Associate to provide the services described in the Services Agreement or to undertake other activities of Business Associate permitted or required by this Agreement or as required by law; provided that such use or disclosure would not violate the Privacy Laws if done by Covered Entity.

(b) Business Associate may use and disclose PHI received by Business Associate in its capacity as Business Associate to Covered Entity as necessary for the proper management and administration of Business Associate, to carry out Business Associate's legal responsibilities or for any other purpose permitted by the HIPAA Laws; provided that Business Associate may only disclose such PHI if the disclosure is permitted by this Agreement and either (i) is required by law, or (ii) Business Associate obtains satisfactory assurances from the person or subcontractor to whom the PHI is disclosed that (A) the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person or subcontractor, and (B) the person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached, or unsecured protected health information is breached as required by 164.410.

(c) When using or disclosing PHI received by Business Associate in its capacity as Business Associate to Covered Entity, Business Associate will make reasonable efforts to limit PHI used or disclosed to the Limited Data Set, as practicable, or to the minimum necessary to accomplish the intended purpose of the use or disclosure; except that Business Associate shall not be required to use or disclose the minimum necessary, as determined in Business Associate's sole discretion, for uses and disclosures made under 45 C.F.R. § 164.502(b)(2).

(d) Business Associate may provide Data Aggregation services relating to the Health Care Operations of Covered Entity.

(e) To the extent Business Associate is to carry out any obligation of Covered Entity under Subpart E of 45 CFR Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation.

3. <u>Safeguards Against Misuse of PHI.</u>

(a) Business Associate will implement appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by this Agreement.

(b) Business Associate will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, availability, and integrity of Electronic PHI created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity as required under 45 C.F.R. §§164.308, 164.310 and 164.312. Such safeguards will (i) protect against reasonably anticipated (A) threats or hazards to the security or integrity of Electronic PHI and (B) uses or disclosures of Electronic PHI that are not permitted or required under the HIPAA Laws, and (ii) ensure compliance with the HIPAA Laws by Business Associate's workforce. Business Associate will encrypt end user devices (e.g., desktops, laptops, smart phones, tablets, etc.) or removable storage media (e.g., USB flash drives, memory cards, external hard drives, writeable CDs or DVDs, backup tapes, etc.) that store Electronic PHI.

(c) Business Associate will not directly or indirectly receive remuneration in exchange for PHI of an individual except as authorized by the HIPAA Laws.

(d) Business Associate will comply with Covered Entity’s Notice of Privacy Practices, and Covered Entity will notify Business Associate of any restrictions agreed to by Covered Entity with respect to any individual’s PHI, to the extent such restriction may impact Business Associate. Covered Entity’s Notice of Privacy Practices is posted on Covered Entity’s website.

(e) Business Associate will not store or transmit Covered Entity’s PHI or Electronic PHI

outside of the United States.

4. Reporting to Covered Entity.

(a) Business Associate will report to Covered Entity any use or disclosure of PHI not permitted by this Agreement of which it becomes aware.

(b) Following discovery of a Breach of Unsecured PHI, Business Associate will report the Breach to Covered Entity no later than twenty-four (24) hours after discovery of the Breach as provided in Section 13 of this Agreement related to notices.

(i) The notification will include, to the extent known, (A) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed during the Breach; and (B) a brief description of what happened (including the date of the Breach and the date of discovery of the Breach), a description of the types of Unsecured PHI that were involved in the Breach, steps individuals should take to protect themselves from potential harm resulting from the Breach, and a brief description of what Business Associate is doing to investigate the Breach, mitigate harm to individuals, and protect against further Breaches.

(ii) If the information required in Section 4(b)(i) of this Agreement is not known at the time of notification to Covered Entity by Business Associate, the information shall be provided as promptly thereafter as the Information becomes available.

(c) Business Associate will report to Covered Entity any Security Incident involving Electronic PHI of which it becomes aware in accordance with the following procedures:

(i) For successful Security Incidents (those that result in unauthorized access, use, disclosure, modification or destruction of information or interference with system operations), Business Associate promptly will report to Covered Entity any successful Security Incidents of which it becomes aware.

(ii) For unsuccessful Security Incidents (those that do not result in unauthorized access, use, disclosure, modification or destruction of information or interference with system operations), Covered Entity and Business Associate agree that this paragraph constitutes notice of such Unsuccessful Security Incidents. By way of example, the Parties consider the following to be illustrative of Unsuccessful Security Incidents when they do not result in actual unauthorized access, use, disclosure, modification or destruction of Electronic PHI or interference with an information system that contains or processes Electronic PHI: (A) pings on a firewall, (B) port scans, (C) attempts to log on to a system or enter a database with an invalid password or username, (D) denial-of-service attacks that do not result in a server being taken off-line, and (E) Malware (worms, viruses, etc.)

(d) Business Associate will take reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of any use or disclosure of PHI by Business Associate or its agents or subcontractors in violation of the requirements of this Agreement.

5. Agreements with Agents or Subcontractors. Business Associate will ensure that any agents (including subcontractors) to whom it 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 and to implement reasonable and appropriate safeguards to protect any PHI that such agent

or subcontractor creates, receives, maintains, or transmits on behalf of Business Associate or Covered Entity.

6. Access to PHI by Individuals.

(a) Upon request from Covered Entity, Business Associate agrees to furnish Covered Entity with copies of the PHI maintained by Business Associate in accordance with procedures established by 45 C. F. R. § 164.524.

(b) In the event an individual or the individual's personal representative makes a request directly to Business Associate for access to the individual's PHI, Business Associate will promptly forward the request to Covered Entity and Covered Entity will be solely responsible for responding to and acting on the request.

(c) If Business Associate uses or maintains PHI in an Electronic Health Record, upon request of an individual or individual's personal representative made directly to Business Associate, Business Associate will notify Covered Entity Covered Entity will transmit the individual's PHI in electronic format to the designee named by the individual or personal representative, unless the Parties otherwise agree that Business Associate may transmit the PHI.

7. Amendment of PHI.

(a) Upon request from Covered Entity, and as directed by Covered Entity, Business Associate will promptly amend PHI about an individual in a Designated Record Set that is maintained by or otherwise within the possession of Business Associate in accordance with procedures established by 45 C.F.R. § 164.526.

(b) In the event an individual or individual's personal representative requests that Business Associate amend PHI about the individual in a Designated Record Set, Business Associate will forward such request immediately to Covered Entity and Covered Entity will be solely responsible for responding to and acting on the request.

8. Accounting of Disclosures.

(a) Business Associate will maintain an accounting of disclosures as required by 45 C.F.R. § 164.528, and will, within 30 days of a request by Covered Entity, make such accounting available to Covered Entity to permit Covered Entity to respond to a request for an accounting of disclosures in accordance with 45 C.F.R. § 164.528. Except as otherwise requested by Covered Entity pursuant to 45 C.F.R. §164.528(b)(3) or (b)(4), Business Associate will furnish Covered Entity the following with respect to disclosures of PHI made by it: (i) the date of disclosure; (ii) the name of the entity or person who received PHI, and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure which includes the basis for such disclosure, or in lieu of such statement, a copy of a written request for the disclosure.

(b) Business Associate will maintain an appropriate recordkeeping system to enable it to comply with the documentation requirements of 45 C.F.R. § 164.528, and will retain records of disclosures of PHI by Business Associate in accordance with procedures established by the HIPAA Laws.

(c) In the event an individual delivers a request for an accounting directly to Business Associate, Business Associate will forward such request immediately to Covered Entity

and Covered Entity will be solely responsible for responding to and acting on the request.

(d) If Business Associate uses or maintains PHI in an Electronic Health Record, Business Associate will notify Covered Entity and, upon written approval by Covered Entity, provide an accounting of disclosures made by Business Associate directly to an individual or individual's personal representative who requests such an accounting from Business Associate, which accounting shall include the disclosures required by 45 C.F.R. § 164.528, as modified by 42 USC § 17935.

9. **Availability of Books and Records**. Business Associate will make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Laws.

10. **Term and Termination.**

(a) This Agreement will become effective on the Effective Date and will continue in effect until all obligations of the Parties have been met under the Services Agreement and under this Agreement.

(b) Covered Entity or Business Associate may terminate this Agreement if it (i) determines that the other has breached a material term of this Agreement that is not cured in accordance with the notice of breach and opportunity to cure provisions in the Services Agreement, or (ii) knows of a pattern of activity or practice of the other that constitutes a material breach or violation of the Covered Entity's or Business Associate's, as applicable, obligations under this Agreement that is not cured in accordance with the notice of breach and opportunity to cure provisions in the Services Agreement. If termination is not feasible, the non-breaching Party will report the problem to the Secretary.

(c) Upon termination of this Agreement, to the extent feasible, Business Associate will return or destroy all PHI received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associates maintains in any form and will retain no copies of such information. If return or destruction is not feasible, Business Associate will extend the protections of this Agreement to the PHI and will limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

11. **Effect of Agreement**. This Agreement is a part of and subject to the terms of the Services Agreement. The Parties are independent contractors, and neither party shall be considered the agent of the other unless otherwise required by law. To the extent any terms of this Agreement conflict with any term of the Services Agreement, the terms of this Agreement will govern. In the event of inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Laws, as amended, or their interpretation by any court or regulatory agency of competent authority and jurisdiction over either Party hereto, the HIPAA Laws, as interpreted by such court or agency, will control. Where the provisions of this Agreement are different from those mandated in the HIPAA Laws, but are nonetheless permitted by such rules as interpreted by courts or agencies, the provisions of this Agreement will control.

12. **Regulatory References**. A reference in this Agreement to a section in the HIPAA Laws means the section as then in effect or as may be amended from time to time.

13. **Notices.** All notices, requests and demands or other communications to be given hereunder to a Party will be made to the Party's designated Privacy Officer in addition to the designees identified in the Services Agreement to receive notice related to the contractual agreements between the Parties.

14. **Entire Agreement; No Third Party Beneficiaries; Amendments.** This Agreement is the entire agreement between the Parties concerning its subject matter, supersedes all prior agreements and understandings, whether or not written, and except as expressly stated herein is not intended to confer upon any person other than the Parties any rights or remedies hereunder. This Agreement may not be modified, nor may any provision be waived or amended, except in writing duly signed by authorized representatives of the Parties. The Parties acknowledge that federal laws regarding health information privacy and data security may undergo change from time to time, and hereby agree to amend, upon the mutual agreement of the Parties, this Agreement from time to time as is necessary for Business Associate and Covered Entity to comply with these statutory requirements. Should the Parties fail to, in good faith, agree promptly to reasonable terms and conditions to amend this Agreement, in order to comply with a new or revised law, rule or regulation, Covered Entity may promptly terminate this Agreement and the Services Agreement in accordance with the notice of termination provisions in the Services Agreement.

15. **Waiver; Severability**. A waiver with respect to one event arising under this Agreement will not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events arising hereunder. The Parties acknowledge and agree that any provision of this Agreement that is or becomes unenforceable or illegal shall be deemed stricken from this Agreement, and that all remaining provisions shall remain in force and effect.

16. **Survival.** Upon termination or expiration of this Agreement, Sections 2, 3, 4, 5, 6, 7, 8 and 9 of this Agreement, and other Sections of this Agreement and the exhibits, if any, that expressly or by their nature survive any termination or expiration of this Agreement or that impose any obligations following the termination or expiration of this Agreement, shall continue and survive in full force and effect.

17. **Execution**. Executed and acknowledged by the undersigned, as the duly authorized representatives of the parties hereto, as of the Effective Date.

[Signatures on following page]

Covered Entity	**Business Associate**
_____	_____
Signature	Signature
_____	_____
Printed Name	Printed Name
_____	_____
Title	Title
_____	_____
Date	Date