UNIVERSITY MEDICAL CENTER ("COVERED ENTITY")

HIPAA Business Associate Privacy and Security Agreement

Business Associate Name: _____

RECITALS

The purpose of this BAA is to comply with "Privacy and Security Requirements," which collectively include, the requirements of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (codified at 45 C.F.R. Parts 160, 162, and 164), as amended ("HIPAA"); privacy and security regulations promulgated by the United States Department of Health and Human Services ("DHHS"); Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, as amended ("HITECH Act"); provisions regarding Confidentiality of Alcohol and Drug Abuse Patient Records (codified at 42 C.F.R. Part 2), as amended; and TEX. HEALTH & SAFETY CODE ANN. §§ 81.046, as amended, 181.001 et seq., as amended, 241.151 et seq., as amended, and 611.001 et seq., as amended.

I. Definitions

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:
(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103.

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean University Medical Center.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(d) Protected Health Information ("PHI"). "Protected Health Information" or PHI shall mean individually identifiable health information that is transmitted or maintained in any form or medium.

(e) Required by Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501 and/or Texas state laws and regulations.

II. Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Immediately report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident. Business Associate further agrees to provide Covered Entity with the following information regarding the Security Incident as soon as possible, but no more than five (5) business days after becoming aware of the Security Incident: (1) a brief description of what happened, including the dates the Security Incident occurred and was discovered; (2) a reproduction of the PHI involved in the Security Incident; and (3) a description of whether and how the PHI involved in the Security Incident was rendered unusable, unreadable, or indecipherable to unauthorized individuals either by encryption or otherwise destroying the PHI prior to disposal. If Business Associate determines that it is infeasible to reproduce the PHI involved in the Security Incident, Business Associate agrees to notify Covered Entity in writing of the conditions that make reproduction infeasible and any information Business Associate has regarding the PHI involved.

Business Associate agrees that Covered Entity will review all Security Incidents reported by Business Associate and Covered Entity, in its sole discretion, will take steps in response, to the extent necessary or required by law including, but not limited to, (1) notifying the individual(s) whose PHI was involved in the Security Incident, either in writing, via telephone, through the media, or by posting a notice on Covered Entity's website, or through a combination of those methods, of the Security Incident; (2) providing the individual(s) whose PHI was involved in the Security Incident with credit monitoring and related services for a period of time to be determined by Covered Entity, at no cost to the individual(s); and (3) providing notice of the Security Incident to the Secretary of the United States Department of Health and Human Services ("HHS").

Business Associate agrees to reimburse Covered Entity for all expenses incurred as a result of Business Associate's Security Incidents, including, but not limited to, expenses related to the activities described above. Business Associate agrees that Covered Entity will select the vendors and negotiate the contracts related to said expenses;

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree in writing to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

(e) Within five (5) days of a request by Covered Entity for access to PHI about an individual, make available to Covered Entity such PHI for so long as such information is maintained. In the event any individual requests access to PHI directly from Business Associate, Business Associate shall within three (3) days forward such request to Covered Entity. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;

(f) Upon Covered Entity's request, promptly amend PHI or a record about the individual in a Designated Record Set that is in the custody or control of Business Associate, so that Covered Entity may meet its amendment obligations under 45 C.F.R. § 164.526. If an individual submits a request for amendment to Business Associate, Business Associate shall within three (3) days forward the request to Covered Entity;

(g) Within ten (10) days of notice by Covered Entity to Business Associate that it has received a request for an accounting of disclosures of PHI regarding an individual during the six (6) years prior to the date on which the accounting was requested, make available to Covered Entity such information as is in Business Associate's possession and is required for Covered Entity to make the accounting required by 45 CFR 164.528. At a minimum, Business Associate shall provide Covered Entity with the following information: (a) the date of the disclosure; (b) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (c) a brief description of the PHI disclosed; and (d) a brief statement of the purpose of such

disclosure which includes an explanation of the basis for such disclosure. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall, within two (2) days, forward such request to Covered Entity. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested. Business Associate hereby agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section;

(h) Comply with the requirements of Subpart E of 45 CFR Part 164 that apply to the Covered Entity in the performance of such obligation(s) to the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E;

(i) Make its internal practices, books, and records available to the Covered Entity and to the Secretary for purposes of determining compliance with the HIPAA Rules;

(j) Comply with the Privacy and Security Requirements, which include Federal and State of Texas requirements governing information relating to HIV/AIDS, mental health, and drugs or alcohol treatment or referral;

(k) Not, without written authorization from Covered Entity, perform marketing or fundraising on behalf of Covered Entity, or engage in the types of communications on behalf of Covered Entity that are excepted from the definition of marketing established at 45 C.F.R. § 164.501. If Covered Entity requests and authorizes Business Associate to engage in these activities, Business Associate shall comply with the applicable Provisions of the HITECH Act and the HIPAA Rules;

(l) Not directly or indirectly receive remuneration in exchange for an individual's PHI unless it is pursuant to specific written authorization by the individual or subject to an exception established in the HIPAA Rules; and

(m) Comply with the FTC Red Flag Rules with respect to its use and disclosure of PHI under this Agreement, including but not limited to a written program to prevent, detect, and mitigate identify theft to the extent Business Associate is a Creditor as defined in the Federal Trade Commission's (FTC) Red Flag Rules, as may be amended (16 CFR Part 681).

III. Permitted Uses and Disclosures by Business Associate

(a) Business Associate may only use or disclose protected health information as necessary to provide Services to or on behalf of Covered Entity as provided in the underlying Service Agreement between Covered Entity and Business Associate .

(b) Business Associate may use or disclose protected health information as required by law.

(c) Business Associate agrees to limit uses and disclosures and requests for protected health information to "limited data set" as that term is defined at 45 CFR 164.514(e)(2) or, if needed, to the minimum necessary as defined at 45 CFR 164.502(b) to accomplish the intended purpose of such use, disclosure, or request.

(d) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity.

(e) Business Associate may use PHI to provide data aggregation services to Covered Entity as permitted by 42 CFR 164.502(j)(1).

IV. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) Covered Entity's current HIPAA Notice of Privacy Practices is found at http://www.umchealthsystem.com/index.php/for-patients/notice-of-privacy. Business Associate is responsible to review and comply with the uses and disclosures as set forth in this notice.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information.

(c) Covered Entity shall 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 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

V. Permissible Requests by Covered Entity

(a) Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

(b) Covered Entity may request Business Associate to use or disclose PHI, if applicable and in accordance with the purpose of this Agreement or an agreement for services between Covered Entity and Business Associate, for data aggregation.

VI. Term and Termination

(a) **Term**. The Term of this Agreement shall be effective as of the Effective Date, and shall terminate when all PHI provided to Business Associate by Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) **Termination for Cause**. Business Associate authorizes termination of this Agreement and the underlying Service Agreement if the Covered Entity reasonably determines that Business Associate has violated a material term of this Agreement. Prior to termination, Covered Entity shall provide Business Associate with written notice of the breach and give Business Associate an opportunity to cure the breach. If Business Associate fails to cure the breach within a reasonable time as determined and specified by Covered Entity it its sole discretion, Covered Entity may terminate this Agreement and the underlying Service Agreement.

(c) **Obligations of Business Associate Upon Termination**. Upon termination of this Agreement for any reason, Business Associate shall return or destroy all protected health information that it maintains in any form and shall retain no copies of such information or, if the parties agree that return or destruction is not feasible, Business Associate shall continue to extend the protections of this Agreement to such information and limit further use of the information to those purposes that make the return or destruction of the information not feasible.

(d) **Mitigation**. If Business Associate violates this Agreement or the HIPAA Rules, Business Associate agrees to mitigate any damage caused by such breach.

(e) **Survival**. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

VII. General Terms

(a) **Regulatory References**. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) **Indemnification.** Business Associate agrees to indemnify, defend, and hold harmless, to the extent allowed by law, Lubbock County Hospital District d/b/a University Medical Center and its Board of Managers, Officers, Employees, and Agents (Individually and Collectively "Indemnitees") against any and all losses, liabilities, judgments, governmental fines and penalties, awards, and costs (including costs of investigations, legal fees, and expenses) arising out of or related to:

1. Business Associate's breach of this BAA relating to the Privacy and Security Requirements; or
2. Any negligent or wrongful acts or omissions of Business Associates or its employees, directors, officers, subcontractors, or agents, relating to the Privacy and Security Requirements, including failure to perform their obligations under the Privacy and Security Requirements.

(c) **Amendment**. This Agreement may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties hereto. Notwithstanding the foregoing, to the extent that any relevant provision of HIPAA or the HIPAA Rules is amended in a manner that changes the obligations of Business Associate or Covered Entity provided for in this Agreement, such changes shall be deemed automatically to apply to and to be incorporated by reference into this Agreement. The Parties agree to amend this Agreement from time to time as necessary to reflect their agreement to such changes.

(d) **Severability**. The provisions of this Agreement shall be severable, and if a provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

(e) **No Third Party Beneficiaries**. Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not a party to this Agreement nor imposing any obligations on either Party hereto to persons not a party to this Agreement.

(f) **Entire Agreement**. This Agreement constitutes the entire Agreement between the Parties hereto with respect to the subject matter hereof and supersedes all previous written or oral understandings, Agreements, negotiations, commitments, and any other writing and communication by or between the Parties with respect to the subject matter hereof.

(g) **Interpretation**. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules

(h) **Notices**. Any notice required to be given pursuant to the terms and provisions of this BAA will be in writing and deemed to be given: (a) upon delivery in person, (b) three (3) days after the date deposited with or sent by U.S. Mail (first class, postage paid, return receipt requested), or (c) upon receipt by commercial delivery service, and addressed as follows, or to such address as Covered Entity may subsequently designate to Business Associate in writing:

Lubbock County Hospital District d/b/a University Medical Center
Attn: Privacy Officer
602 Indiana Avenue
Lubbock, Texas 79415

(i) **Inspection**. Upon written request, Business Associate agrees to make available to Covered Entity and its duly authorized representatives during normal business hours Business Associate's internal practices, books, records and documents relating to the use and disclosure of confidential information, including, but not limited to, PHI received from, or created or received on behalf of, Covered Entity in a time and manner designated by Covered Entity for the purposes of Covered Entity determining compliance with the Privacy and Security Requirements. Business Associate agrees to allow such access until the expiration of four (4) years after the services are furnished under the contract or subcontract or until the completion of any audit or audit period, whichever is later. Business Associate agrees to allow similar access to books, records, and documents related to contracts between Covered Entity and organizations related to or subcontracted by Covered Entity to whom Business Associate provides confidential information, including, but not limited to, PHI received from, or created or received on behalf of, Covered Entity.

(j) **No Agency.** Business Associate shall not be deemed to be the common law agent of Covered Entity.

(k) **Assignment.** This Agreement shall be binding upon and shall inure to the benefit of the parties and their respective heirs (as applicable), legal representatives, successors, and permitted assigns. Business Associate shall not have the right to assign or transfer its rights and obligations under this Agreement to any third party without prior written consent of Covered Entity.

(l) **Execution.** This Agreement may be executed in multiple counterparts, each of which shall constitute an original and all of which shall constitute but one Agreement.

(m) **Governing Law.** This Agreement shall be interpreted, construed, and governed according to the laws of the State of Texas. The District Court of Lubbock County, Texas shall be the exclusive forum for the determination of any disputes regarding or related to this Agreement or its performance and the parties irrevocably consent to the personal jurisdiction and venue in such court, provided that, if the District Court of Lubbock County lacks subject matter jurisdiction, exclusive jurisdiction and venue shall be in the court nearest to Lubbock, Texas which has subject matter jurisdiction over the controversy.

(n) **Audit.** Business Associate shall immediately notify Covered Entity's Privacy Officer if Business Associate becomes the subject of a Department of Health and Human Services audit pursuant to 42 USC § 17940.

BUSINESS ASSOCIATE:

By: _____

Printed Name: _____

Title: _____

Effective Date: _____