Model Business Associate Agreement

Instructions:

The Texas Health Services Authority (THSA) has developed a model BAA for use between providers (Covered Entities) and HIEs (Business Associates). The model BAA is **not required** for use by the HIEs. Rather, it was developed to provide a potential aid to reduce negotiating time between HIEs and providers. This model BAA is based on the BAA the Integrated Care Collaboration negotiated with its users. The main changes are the addition of some terms to address requirements under HB 300 (82nd Texas Legislature) and some changes to timeframes included in the document. The model BAA has also been amended to reflect the HIPAA/HITECH Omnibus Rule. This model BAA is not intended to serve as a substitute for legal advice, and HIEs that opt to use this document should consult an attorney to ensure that they use this document in such a way as to make it an enforceable BAA that meets applicable HIPAA and HITECH requirements.

Please note that Chapter 181 of the Texas Health and Safety Code defines the term "Covered Entity" more broadly than does HIPAA in 45 C.F.R. §160.103. The HIPAA definition, rather than the Texas definition, is used in this model BAA, as not all "covered entities" as defined by Texas law are required to comply with HIPAA and HITECH. However, all covered entities as defined by Chapter 181 are required to comply with the applicable Chapter 181 provisions.

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") dated _____, 2013 (the "Effective Date"), is entered into by and between _____ ("Covered Entity") and _____("Business Associate"), each a "Party" and collectively, the "Parties."

Covered Entity and Business Associate have entered into, are entering into, or may subsequently enter into, agreements or other documented arrangements (collectively, the "Business Arrangements") pursuant to which Business Associate may provide products and/or services for Covered Entity that require Business Associate to access, create, maintain, and use health information that is protected by state and/or federal law.

Pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the U.S. Department of Health & Human Services ("HHS") promulgated the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards"), at 45 C.F.R. Parts 160 and 164, requiring certain individuals and entities subject to the Privacy Standards (each a "Covered Entity", or collectively, "Covered Entities") to protect the privacy of certain individually identifiable health information ("Protected Health Information" or "PHI").

Pursuant to HIPAA, HHS issued the Security Standards (the "Security Standards"), at 45 C.F.R. Parts 160, 162 and 164, for the protection of electronic protected health information ("EPHI").

In order to protect the privacy and security of PHI, including EPHI, created or maintained by or on behalf of the Covered Entity, the Privacy Standards and Security Standards require a Covered Entity to enter into a "business associate agreement" with certain individuals and entities providing services for or on behalf of the Covered Entity if such services require the use or disclosure of PHI or EPHI.

On February 17, 2009, the federal Health Information Technology for Economic and Clinical Health Act was signed into law (the "HITECH Act"), and the HITECH Act imposes certain privacy and security obligations on Covered Entities in addition to the obligations created by the Privacy Standards and Security Standards.

The HITECH Act revises many of the requirements of the Privacy Standards and Security Standards concerning the confidentiality of PHI and EPHI, including extending certain HIPAA and HITECH Act requirements directly to Business Associates.

The HITECH Act requires that certain of its provisions be included in business associate agreements, and that certain requirements of the Privacy Standards be imposed contractually upon Covered Entities as well as Business Associates.

The Texas Legislature has adopted certain privacy and security requirements that are more restrictive than those required by HIPAA and HITECH, and such requirements are applicable to Business Associates as "Covered Entities" as defined by Texas law; and

Because Business Associate and Covered Entity desire to enter into this Business Associate Agreement, in consideration of the mutual promises set forth in this Agreement and the applicable Business Arrangements, and other good and valuable consideration, the sufficiency and receipt of which are hereby acknowledged, the Parties agree as follows:

1. Business Associate Obligations. Business Associate may receive from Covered Entity, or create or receive or maintain on behalf of Covered Entity, health information that is protected under applicable state and/or federal law, including without limitation, PHI and EPHI. All references to PHI herein shall be construed to include EPHI. Business Associate agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the Privacy Standards, Security Standards the HITECH Act, or Texas law, including without limitation the provisions of Texas Health and Safety Code Chapters 181 and 182 as amended by HB 300 (82nd Legislature), effective September 1, 2012, in each case including any implementing regulations as applicable (collectively referred to hereinafter as the "Confidentiality Requirements") if the PHI were used or disclosed by Covered Entity in the same manner.

2. Use of PHI. Except as otherwise required by law, Business Associate shall use PHI in compliance with 45 C.F.R. § 164.504(e). Furthermore, Business Associate shall use PHI (i) solely for Covered Entity's benefit and only for the purpose of performing services for Covered Entity as such services are defined in Business Arrangements, (ii) for Data Aggregation Services (as hereinafter defined), and (iii) as necessary for the proper management and administration of the Business Associate or to carry out its legal responsibilities, provided that such uses are permitted under federal and state law. For avoidance of doubt, under no circumstances may Business Associate sell PHI in such a way as to violate Texas Health and Safety Code, Chapter 181.153, as amended by HB 300 (82nd Legislature), effective September 1, 2012, nor shall Business Associate use PHI for marketing purposes in such as manner as to violate Texas Health and Safety Code Section 181.152, or attempt to re-identify any information in violation of Texas Health and Safety Code Section 181.151, regardless of whether such action is on behalf of or permitted by the Covered Entity.

To the extent not otherwise prohibited in the Business Arrangements or by applicable law, use, creation and disclosure of de-identified health information, as that term is defined in 45 CFR § 164.514, by Business Associate is permitted.

3. Disclosure of PHI. Subject to any limitations in this Agreement, Business Associate may disclose PHI to any third party persons or entities as necessary to perform its obligations under the Business Arrangement and as permitted or required by applicable federal or state law. Business Associate recognizes that under the HIPAA/HITECH Omnibus Final Rule, Business Associates may not disclose PHI in a way that would be prohibited if Covered Entity made such a disclosure. Any disclosures made by Business Associate will comply with minimum necessary requirements under the Privacy Rule and related regulations.

3.1 Business Associate shall not [and shall provide that its directors, officers, employees, subcontractors, and agents, do not] disclose PHI to any other person (other than members of their respective workforce as specified in subsection 3.1(ii) below), unless disclosure is required by law or authorized by the person whose PHI is to be disclosed. Any such disclosure other than as specifically permitted in the immediately preceding sentences shall be made only if such disclosee has previously signed a written agreement that:

(i) Binds the disclosee to the provisions of this Agreement pertaining to PHI, for the express benefit of Covered Entity, Business Associate and, if disclosee is other than Business Associate, the disclosee;

(ii) Contains reasonable assurances from disclosee that the PHI will be held confidential as provided in this Agreement, and only disclosed as required by law for the purposes for which it was disclosed to disclosee; and

(iii) Obligates disclosee to immediately notify Business Associate of any breaches of the confidentiality of the PHI, to the extent disclosee has obtained knowledge of such breach.

3.2 Business Associate shall not disclose PHI to any member of its workforce and shall provide that its subcontractors and agents do not disclose PHI to any member of their respective workforces, unless Business Associate or such subcontractor or agent has advised such person of Business Associate's obligations under this Agreement, and of the consequences for such person and for Business Associate or such subcontractor or agent of violating them as memorialized in a business associate agreement pursuant to the HIPAA/HITECH Omnibus Final Rule. Business Associate shall take and shall provide that each of its subcontractors and agents take appropriate disciplinary action against any member of its respective workforce who uses or discloses PHI in contravention of this Agreement.

3.3 In addition to Business Associate's obligations under Section 9, Business Associate agrees to mitigate, to the extent commercially practical, harmful effects that are known to Business Associate and is the result of a use or disclosure of PHI by Business Associate or Recipients in violation of this Agreement.

4. <u>Access to and Amendment of Protected Health Information</u>. Business Associate shall (i) provide access to, and permit inspection and copying of, PHI by Covered Entity; and (ii) notify Covered Entity within 5 business days of any request for amendment or access received from the individual. The decision to grant or deny the amendment shall be made solely by Covered Entity. Any such amendments shall be made in such a way as to record the time and date of the change, if feasible, and in accordance with any subsequent requirements promulgated by the Texas Medical Board with respect to amendment of electronic medical records. If the amendment is granted, Covered Entity shall submit updated records to Business Associate within ___ business days. Business Associate shall respond to any request from Covered Entity for access by an individual within seven (7) days of such request. Business Associate may charge a reasonable fee based upon the Business Associate's labor costs in responding to a request for electronic information (or the fee approved by the Texas Medical Board for the production of non-electronic media copies).

5. Accounting of Disclosures. Business Associate shall make available to Covered Entity in response to a request from an individual, information required for an accounting of disclosures of PHI with respect to the individual in accordance with 45 CFR § 164.528, as amended by Section 13405(c) of the HITECH Act and any related regulations or guidance issued by HHS in accordance with such provision.

6. Records and Audit. Business Associate shall make available to the United States Department of Health and Human Services or its agents, its internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by Business Associate on behalf of Covered Entity for the purpose of determining Covered Entity's compliance with the Confidentiality Requirements or the requirements of any other health oversight agency, in a time and manner designated by the Secretary.

7. Implementation of Security Standards; Notice of Security Incidents. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as expressly permitted under this Agreement. Business Associate will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate acknowledges that the HITECH Act requires Business Associate to comply with 45 C.F.R. §§164.308, 164.310, 164.312 and 164.316 as if Business Associate were a Covered Entity, and Business Associate agrees to comply with these provisions of the Security Standards and all additional security provisions of the HITECH Act.

Furthermore, to the extent feasible, Business Associate will use commercially reasonable efforts to secure PHI through technology safeguards that render such PHI unusable, unreadable and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with HHS Guidance published at 74 Federal Register 19006 (April 17, 2009), or such later regulations or guidance promulgated by HHS or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as PHI. Lastly, Business Associate will promptly report to Covered Entity any successful Security Incident of which it becomes aware. At the request of Covered Entity, Business Associate shall identify: the date of the Security Incident, the scope of the Security Incident, the Business Associate's response to the Security Incident and the identification of the party responsible for causing the Security Incident, if known.

8. Data Breach Notification and Mitigation.

8.1 HIPAA Data Breach Notification and Mitigation. Business Associate agrees to implement reasonable systems for the discovery and prompt reporting to Covered Entity of any "breach" of "unsecured PHI" as those terms are defined by 45 C.F.R. § 164.402. Specifically, a breach is an unauthorized acquisition, access, use or disclosure of unsecured PHI, including ePHI, which compromises the security or privacy of the PHI/ePHI. A breach is presumed to have occurred unless there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed in 45 C.F.R. § 164.402(2)(i)-(iv) (hereinafter a "HIPAA Breach"). The parties acknowledge and agree that 45 C.F.R. § 164.404, as described below in this Section 8.1, governs the determination of the

date of discovery of a HIPAA Breach. In addition to the foregoing and notwithstanding anything to the contrary herein, Business Associate will also comply with applicable state law, including without limitation, Section 521 Texas Business and Commerce Code, as amended by HB 300 (82nd Legislature), or such other laws or regulations as may later be amended or adopted. In the event of any conflict between this Section 8.1, the Confidentiality Requirements, Section 521 of the Texas Business and Commerce Code, and any other later amended or adopted laws or regulations, the most stringent requirements shall govern.

8.2 Discovery of Breach. Business Associate will, following the discovery of a HIPAA Breach, notify Covered Entity without unreasonable delay and in no event later than the earlier of the maximum of time allowable under applicable law or three (3) business days after Business Associate discovers such HIPAA Breach, unless Business Associate is prevented from doing so by 45 C.F.R. §164.412 concerning law enforcement investigations. For purposes of reporting a HIPAA Breach to Covered Entity, the discovery of a HIPAA Breach shall occur as of the first day on which such HIPAA Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. Business Associate will be considered to have had knowledge of a HIPAA Breach if the HIPAA Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the HIPAA Breach) who is an employee, officer or other agent of the Business Associate.

8.3 Reporting a Breach. Without unreasonable delay and no later than the earlier of the maximum of time allowable under applicable law or five (5) business days following a HIPAA Breach, Business Associate shall provide Covered Entity with sufficient information to permit Covered Entity to comply with the HIPAA Breach notification requirements set forth at 45 C.F.R. § 164.400 *et seq.* Specifically, if the following information is known to (or can be reasonably obtained by) the Business Associate, Business Associate will provide Covered Entity with:

(i) contact information for individuals who were or who may have been impacted by the HIPAA Breach (e.g., first and last name, mailing address, street address, phone number, email address);

(ii) a brief description of the circumstances of the HIPAA Breach, including the date of the HIPAA Breach and date of discovery;

(iii) a description of the types of unsecured PHI involved in the HIPAA Breach (e.g., names, social security number, date of birth, addressees, account numbers of any type, disability codes, diagnostic and/or billing codes and similar information);

(iv) a brief description of what the Business Associate has done or is doing to investigate the HIPAA Breach, mitigate harm to the individual impacted by the HIPAA Breach, and protect against future HIPAA Breaches; and

(v) appoint a liaison and provide contact information for same so that Covered Entity may ask questions or learn additional information concerning the HIPAA Breach.

Following a HIPAA Breach, Business Associate will have a continuing duty to inform Covered Entity of new information learned by Business Associate regarding the HIPAA Breach, including but not limited to the information described in items (i) through (v), above.

9. Termination.

9.1 This Agreement shall commence on the Effective Date.

9.2 Upon the termination of the applicable Business Arrangement, either Party may terminate this Agreement by providing written notice to the other Party.

9.3 Upon termination of this Agreement for any reason, Business Associate agrees:

(i) to return to Covered Entity or to destroy all PHI received from Covered Entity or otherwise through the performance of services for Covered Entity, that is in the possession or control of Business Associate or its agents. Business Associate agrees that all paper, film, or other hard copy media shall be shredded or destroyed such that it may not be reconstructed, and EPHI shall be purged or destroyed concurrent with NIST Guidelines for media sanitization at http://www.csrc.nist.gov/; or

(ii) in the case of PHI which is not feasible to "return or destroy," to 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. Business Associate further agrees to comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment of such PHI.

10. Miscellaneous.

10.1 Notice. All notices, requests, demands and other communications required or permitted to be given or made under this Agreement shall be in writing, shall be effective upon receipt or attempted delivery, and shall be sent by (i) personal delivery; (ii) certified or registered United States mail, return receipt requested; (iii) overnight delivery service with proof of delivery; or (iv) facsimile with return facsimile acknowledging receipt. Notices shall be sent to the addresses below. Neither party shall refuse delivery of any notice hereunder.

Covered Entity:

_____

_____

_____

_____

Business Associate:

_____
_____
_____
_____

10.2 Waiver. No provision of this Agreement or any breach thereof shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

10.3 Assignment**.** Neither Party may assign (whether by operation or law or otherwise) any of its rights or delegate or subcontract any of its obligations under this Agreement without the prior written consent of the other Party. Notwithstanding the foregoing, Covered Entity shall have the right to assign its rights and obligations hereunder to any entity that is an affiliate or successor of Covered Entity, without the prior approval of Business Associate.

10.4 Severability. Any provision of this Agreement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

10.5 Entire Agreement. This Agreement constitutes the complete agreement between Business Associate and Covered Entity relating to the matters specified in this Agreement, and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. In the event of any conflict between the terms of this Agreement and the terms of the Business Arrangements or any such later agreement(s), the terms of this Agreement shall control unless the terms of such Business Arrangements are more strict with respect to PHI and comply with the Confidentiality Requirements, or the parties specifically otherwise agree in writing. No oral modification or waiver of any of the provisions of this Agreement shall be binding on either Party; provided, however, that upon the enactment of any law, regulation, court decision or relevant government publication and/or interpretive guidance or policy that the Covered Entity believes in good faith will adversely impact the use or disclosure of PHI under this Agreement, Covered Entity may amend the Agreement to comply with such law, regulation, court decision or government publication, guidance or policy by delivering a written amendment to Business Associate which shall be effective thirty (30) days after receipt. No obligation on either Party to enter into any transaction is to be implied from the execution or delivery of this Agreement. This Agreement is for the benefit of, and shall be binding upon the parties, their affiliates and respective successors and assigns. No third party shall be considered a third-party beneficiary under this Agreement, nor shall any third party have any rights as a result of this Agreement.

10.6 Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of the state of Texas. Venue for any dispute relating to this Agreement shall be in Travis County, Texas.

10.7 Nature of Agreement; Independent Contractor. Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the parties or any of their affiliates, or (ii) a relationship of employer and employee between the parties. Business Associate is an independent contractor, and not an agent of Covered Entity. This Agreement does not express or imply any commitment to purchase or sell goods or services.

10.8 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document. In making proof of this Agreement, it shall not be necessary to produce or account for more than one such counterpart executed by the party against whom enforcement of this Agreement is sought. Signatures to this Agreement transmitted by facsimile transmission, by electronic mail in portable document format (".pdf") form, or by any other electronic means intended to preserve the original graphic and pictorial appearance of a document, will have the same force and effect as physical execution and delivery of the paper document bearing the original signature.

10.9 Definitions. For the purposes of this Agreement, the following definitions shall apply:

(i) *"Business Associate"* shall have the meaning given to the term "Associate" under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

(ii) *"Covered Entity"* shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

(iii) "*Data Aggregation Services*" shall mean the combining of PHI or EPHI by Business Associate with the PHI or EPHI 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, payment to, and treatment of patients by the respective covered entities.

(iv) *"Electronic Protected Health Information"* or *"EPHI"* shall have the meaning given to such term under the HIPAA Rule, including but not limited to 45 CFR Parts 160, 162, and 164, and under HITECH.

(v) *"Privacy Rule"* shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160, 162 and 164.

(vi) *"Security Rule"* shall mean the HIPAA regulation that is codified at 45 C.F.R. Part 164.

(vii) *"Protected Health Information"* or *"PHI"* means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental 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 (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 164.501. *[45 CFR §§160.103 and 164.501.*

(viii) The Health Information Technology for Economic and Clinical Health ("HITECH") Act shall mean Division A, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5). The U.S. Department of Health and Human Services ("HHS") omnibus final rule at 78 Fed. Reg. 5555-5702 implements the privacy, security, enforcement, and breach notice provisions of HITECH.

(ix) Any other capitalized term not otherwise defined in this Section 13.10 or this Agreement shall have the meanings set forth in the Privacy Standards, Security Standards or the HITECH Act, as applicable.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
_____	_____
By:_____	By_____
Title:_____	Title:_____
Date:_____	Date:_____