MANAGED IT SERVICES

HIPAA COMPLIANCE

(PRIVACY AND SECURITY OF HEALTH INFORMATION)

This BUSINESS ASSOCIATE AGREEMENT ("Agreement") is entered into on _____, 20_____ between TechWorks, Inc. ("Business Associate") and _____ ("Provider"). Both parties agree as follows:

I. DEFINITIONS

Capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Standards for Privacy of Individually Identifiable Health Information, at 45 Code of Federal Regulations ("CFR") part 160 and part 164 subpart E (the "Privacy Rule"), the Security Standards issued at 45 CFR part 160 and part 164 subpart C (the "Security Rule"), and the breach notification rules at 45 CFR Part 164, subpart D ("Breach Rules") as they may be amended from time to time.

The following capitalized terms shall have the following meaning when used in this Agreement:

a) "Breach" shall have the same meaning as the term "Breach" in 45 CFR 164.402.
b) "Designated Record Set" shall mean a group of records maintained for Provider that are the medical and/or billing records that refer to an individual Patient.
c) "Electronic PHI" shall mean the PHI that is transmitted or maintained by Business Associate on behalf of Provider in electronic media, including, but not limited to, hard drives, disks, on the internet, or on an intranet.
d) "HITECH Act" shall mean the "Health Information Technology for Economic and Clinical Health Act" set forth within P.L. 111-5, and all relevant regulations promulgated thereunder, as amended from time to time.
e) "Patient" shall mean the individual whose PHI is contained in a specific medical or billing record that Business Associate maintains on behalf of Provider or that person's duly appointed guardian or qualified personal representative.
f) "PHI" shall have the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on the behalf of Provider.
g) "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his designee.
h) "Unsecured PHI" shall have the same meaning as the term "Unsecured Protected Health Information" as defined in 45 CFR 164.402.

II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a) Business Associate agrees to comply with those provisions of the Security Rule that are set forth at 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316, as amended from time to time, with respect the security of PHI, in the same manner that such regulations apply to the Provider.
b) Business Associate agrees to comply with the Privacy Rule at 45 C.F.R. § 164.504(e), as amended from time to time, with respect to its use and disclosure of PHI, in the same manner that such regulation applies to Provider. The additional requirements of the HITECH Act that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to Business Associate and shall be and by this reference hereby are incorporated into the Business Associate Agreement.
c) Business Associate agrees to not use or further disclose PHI other than as specifically permitted or required by this Agreement or as required by law.
d) Business Associate agrees to use appropriate safeguards and comply, where applicable, with Subpart C of 45 CFR Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement.
e) Business Associate agrees to 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 the Agreement.
f) Business Associate agrees to report to Provider if it becomes aware of any use or disclosure of PHI not provided for by this Agreement, including any Breach of Unsecured PHI as required by 45 CFR 164.410, and any Security Incident of which it becomes aware. Notwithstanding anything herein to the contrary, the parties acknowledge and agree that this Agreement shall constitute notice to Provider that Business Associate may periodically experience broadcast attacks on its firewall, port scans, unsuccessful log-on attempts, denials of service and similar unsuccessful security incidents, and Business Associate need not further report such incidents to Provider so long as such incidents do not result in unauthorized access, use or disclosure of PHI.
g) Business Associate agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate on behalf of Provider agree to the same restrictions and conditions that apply to Business Associate with respect to such information, including, without limitation, implementation of appropriate safeguards to protect the security of Electronic PHI.
h) Upon the written request of Provider, Business Associate agrees to provide access to Provider to PHI that Business Associate maintains in a Designated Record Set (if in fact its arrangements with Provider require Business Associate to maintain Designated Record Sets on behalf of Provider), in order for Provider to meet the Patient access and copying requirements under 45 CFR 164.524. If Business Associate maintains an electronic health record which contains the PHI, Business Associate shall provide such information produced in accordance with this section 2(h) in electronic format to enable Provider to fulfill its obligations under applicable regulations.
i) Upon the written request of Provider, Business Associate agrees to make any amendment(s) to PHI that Business Associate maintains in a Designated Record Set (if in fact its arrangements with Provider require Business Associates to maintain Designated Record Sets on behalf of Provider), that the Provider directs or agrees to pursuant to 45 CFR 164.526.
j) Business Associate agrees to make its internal practices, books and records relating to the use and disclosure of PHI available at the request of the Provider to the Secretary, for purposes of determining Provider's compliance with the Privacy Rule, subject to attorney-client or other applicable legal privileges.
k) Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Provider to respond to a request by Patient for an accounting of disclosures of PHI in accordance with 45 CFR 164.528, as may be amended from time to time.
l) Upon written request of Provider, Business Associate agrees to provide Provider with information collected in accordance with Section II.i. of this Agreement to permit Provider to respond to a request by Patient for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

m) Business Associate agrees that to the extent it is to carry out Provider's obligation under the Privacy Rule that it will comply with the requirements of the Privacy Rule that apply to Provider in the performance of such obligation.
n) Business Associate agrees to notify Provider without unreasonable delay, but in no event more than 60 days after Business Associate becomes aware of an unauthorized use or disclosure by or on behalf of Business Associate which constitutes a Breach of Unsecured PHI unless it receives a request to delay such notification from a law enforcement official pursuant to 45 CFR 164.412. Such notification shall include a list of impacted Patients, and describe the Breach in such reasonable detail.
o) Upon written request of Provider, Business Associate will comply with a Patient request for restriction of certain disclosures to health plans in accordance with 45 CFR 164.522 and the HITECH Act, if the disclosure is to a health care plan for the purposes of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which Patient has paid for out of pocket in full. Except to the extent that Provider must agree to a Patient request for restriction under the HITECH Act, Business Associate shall not be required to comply with a Patient's request to restrict the use or disclosure of PHI.

III. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

a) Business Associate may use or disclose PHI to perform functions, activities or services for, or on behalf of, Provider, in accordance with the contractual or other arrangements between Provider and Business Associate.
b) Except as otherwise specifically permitted by Section IV. of this Agreement, Business Associate shall limit its use and disclosure of PHI to only the minimum necessary PHI required by Business Associate to furnish services on behalf of Provider.

IV. SPECIFIC USE AND DISCLOSURE PROVISIONS

a) Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
b) Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom PHI is disclosed that it will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of PHI has been breached.
c) Business Associate may use PHI to provide data aggregation services as permitted by 45 CFR 164.504(e)(2)(i)(B) (i.e. the combining PHI received from Provider with PHI received by Business Associate in its capacity as the business associate of another practice for the purpose of conducting data analyses that relate to health care operations of various practices).
d) Business Associate may use PHI to create de-identified health information to the extent permitted by the Privacy Rule. There will be no restrictions on Business Associate's use or disclosure of the de-identified health information once it is so de-identified.

V. OBLIGATIONS OF PROVIDER

a) Provider represents and warrants to Business Associate that its Notice of Privacy Practices permits Provider to disclose PHI to Business Associate, and that the Notice of Privacy Practices used by Provider incorporates the terms and statements required by the Privacy Rule. Provider agrees that Provider shall not modify such notice or its privacy procedures in any manner that may affect Business Associate's authority to use or disclose PHI pursuant to this Agreement without the consent of Business Associate, except as may be required by applicable law.
b) If applicable, Provider shall notify Business Associate of any changes in, or revocation of, permission by a Patient to use or disclose PHI, to the extent that such changes may affect the permitted uses or disclosures of such PHI by Business Associate.

c) Provider shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under the Privacy Rule, Security Rule or other applicable law or its Notice of Privacy Practices if done by Provider except the uses specifically permitted under Section IV. above, where Business Associate may use or disclose PHI for data aggregation or management and administrative activities of Business Associate.
d) Provider represents and warrants to Business Associate that Provider shall comply with all requirements of the Privacy Rule, Security Rule, and any similar federal or state requirements relating to privacy concerns.

VI. MUTUAL OBLIGATIONS

a) The parties agree that they will neither directly nor indirectly receive remuneration in exchange for any PHI of a Patient, unless a valid authorization, pursuant to 45 CFR 164.508, is executed by that Patient. Notwithstanding the foregoing, the parties agree that they may receive remuneration in exchange for PHI of a patient in accordance with 42 USC § 17935(d)(2) and 45 CFR 164.502(a)(5)(ii)(B)(2).

VII. TERM AND TERMINATION

a) The Term of this Agreement shall be effective as of the date set forth above, and shall remain effective so long as a relationship between the Provider and the Business Associate shall persist. This Agreement shall terminate when all of the PHI provided by Provider to Business Associate or created or received by Business Associate on behalf of Provider is destroyed or returned to Provider or, if it is infeasible to return or destroy PHI, protections are extended to such information in accordance with the termination provisions in Section VII.d.2. below.
b) Upon Provider's knowledge of a material breach of this Agreement by Business Associate, Provider shall provide written notice to Business Associate identifying the breach, and permit the Business Associate 30 days to cure the breach; if Business Associate does not cure the breach or end the violation within the time specified, or if cure is not possible, Provider may immediately terminate this Agreement, and/or report the event to the Secretary.

c) Upon Business Associate's knowledge of a material breach of this Agreement by the Provider, the Business Associate shall provide written notice to the Provider identifying the breach, and may permit the Provider the opportunity to cure the breach within 30 days; if Provider does not cure the breach or end the violation within the time specified, or if cure is not possible, Business Associate may immediately terminate this Agreement, and/or report the event to the Secretary.
d) Effect of Termination.
    1. Except as provided in Section VII.d.2. below, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Provider, or created or received by Business Associate on behalf of Provider. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.
    2. In the event the Business Associate determines that the returning of or destroying of the PHI is infeasible, Business Associate shall provide to Provider notification of the conditions that make return or destruction infeasible, and thereafter, 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.

VIII. NOTICE

a) Any and all notices, requests, or reports, required or permitted to be given under any provision of this Agreement shall be in writing and shall be deemed given upon the mailing thereof by first

class certified mail, return receipt requested, postage prepaid, or by overnight mail. If such notice is to the Business Associate, then it shall be sent to the attention of the HIPAA Compliance Officer at the address provided below with a copy to the General Counsel, TechWorks, Inc., 324 Alhambra Blvd, Sacramento CA 95816. If such notice is to the Provider, then it shall be sent to the address that the Business Associate then has on file for the Provider.

IX. MISCELLANEOUS

a) This Agreement is between Provider and Business Associate and shall not be construed, interpreted, or deemed to confer any rights whatsoever to any third party, including Patients.
b) The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with Health Insurance Portability and Accountability Act, the Transaction Standards, Security Standards, the Privacy Rules, and the HITECH Act.
c) This Agreement shall be governed by and construed in accordance with the laws of the state of California, without regard to the conflicts of law principles of such state.
d) Provider and Business Associate agree to negotiate in good faith if, in either party's reasonable judgment, modification of this Agreement becomes necessary due to legislative or regulatory amendments to the Privacy Rule, the Security Rule, or the HITECH Act.
e) In the event that it is impossible to comply with both this Agreement and any underlying services agreements between the parties, the provisions of this Agreement shall control with respect to those provisions of each agreement that expressly conflict.
f) This agreement replaces and supersedes any previous agreement with respect to the subject matter hereof.

AGREED AND ACCEPTED:

Date:	**Date:**
Business Associate: TechWorks Inc	**Provider:**
Signature:	**Signature:**
Name:	**Name:**
Title: HIPAA Compliance Officer	**Title:**