

## HIPAA AGREEMENT

This HIPAA Agreement is entered into by and between HB Computers ("HB Computers"), of 17131 Beach Blvd Suite B, Huntington Beach, CA 92647 and \_\_\_\_\_ ("Hospital/Doctor"), of {Address}, \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_, (each "Party", collectively "Parties").

The Parties have a prior written agreement, dated \_\_\_\_\_, ("the Primary Agreement") under which the Hospital/Doctor regularly receives, uses and/or discloses Protected Health Information in its performance of the services described in the Primary Agreement. This Agreement sets forth the obligations and agreements of the Parties relating to compliance with the Standards for Privacy of Individually Identifiable Health Information ("the Privacy Regulation"), 45 C.F.R. Parts 160 and 164, and the Security Regulations (45 C.F.R. Parts 160, 162, and 164), promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health ("HITECH"), and the California statutes governing social security numbers, I.C. 4-1-10-1 et. seq. This Agreement applies to all Protected Health Information created or received by Hospital/Doctor from HB Computers or from another person or entity on behalf of HB Computers, and governs how such Protected Health Information may be used or disclosed.

The Parties hereby agree as follows:

### 1. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

1.1 Hospital/Doctor shall be permitted to use and disclose Protected Health Information created or received on behalf of HB Computers for all purposes necessary to provide the services and to perform its obligations under the Primary Agreement, provided that said use and disclosure comply with the requirements of HIPAA. Hospital/Doctor acknowledges that under the requirements of HITECH, the HIPAA Privacy and Security Regulations apply to Hospital/Doctors and the additional privacy requirements outlined in HITECH apply to Hospital/Doctor to the same extent that they apply to covered entities under HIPAA. The requirements of the HITECH statutes are incorporated herein by reference. In accordance with the applicable requirements of HITECH, any uses or disclosures of PHI must be limited, to the extent practicable, to the Limited Data Set, or, if needed to accomplish the purposes of this Agreement, to the minimum necessary to accomplish the intended purpose of such use or disclosure.

1.2 Subject to paragraph 1.1, Hospital/Doctor may use Protected Health Information created or received by Hospital/Doctor from or on behalf of HB Computers, if necessary, for the proper management and administration of the Hospital/Doctor and to fulfill any current or future legal responsibilities of the Hospital/Doctor.

1.3 Subject to paragraph 1.1, Hospital/Doctor may disclose Protected Health Information created or received by Hospital/Doctor on behalf of HB Computers, if necessary, for the proper management and

administration of the Hospital/Doctor and to fulfill any current or future legal responsibilities of the Hospital/Doctor, provided:

1.3.1 The disclosure is Required by California State Law, or

1.3.2 Hospital/Doctor obtains satisfactory assurances from the person or entity to whom the Protected Health Information is disclosed that (i) the Protected Health Information will be held confidentially and used or further disclosed only as Required by California State Law or for the purpose for which it was disclosed to the person or entity; and (ii) the Hospital/Doctor will be notified of any instances of which the person is aware in which the confidentiality of the information is breached.

1.3.3 As of the effective date of the applicable HITECH regulations, Hospital/Doctor shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual unless Hospital/Doctor has obtained from the individual a valid authorization that includes specification of whether the Protected Health Information can be further exchanged for remuneration by the Hospital/Doctor.

## **2. RESPONSIBILITIES OF HOSPITAL/DOCTOR WITH RESPECT TO PROTECTED HEALTH INFORMATION**

2.1 Hospital/Doctor agrees not to use or disclose Protected Health Information except as expressly permitted by this Agreement, HIPAA, or as required by California State Law.

2.2 Hospital/Doctor hereby agrees to maintain the security and privacy of all Protected Health Information in a manner consistent with California and Federal laws and regulations, including but not limited to the HIPAA Privacy Regulations and the Security Regulations (45 C.F.R. Parts 160, 162, and 164) and HITECH, and I.C. 4-1-10-1 et. seq. and Hospital/Doctor further agrees to use appropriate safeguards and security procedures to prevent use or disclosure of Protected Health Information not permitted by this Agreement.

2.3 Hospital/Doctor shall not disclose Protected Health Information to any member of its workforce unless such member of its workforce has a need to use such Protected Health Information, and Hospital/Doctor has advised such person of Hospital/Doctor's privacy and security obligations under this Agreement, including the consequences for violation of such obligations. Hospital/Doctor shall take two appropriate disciplinary actions against any member of its workforce who uses or disclose Protected Health Information in violation of this Agreement or California State law.

2.4 Hospital/Doctor shall require all its subcontractors and agents that receive or use, or have access to, Protected Health Information under this Agreement to agree, in writing, to adhere to the same restrictions and conditions on the use or disclosure of Protected Health Information that apply to the Hospital/Doctor pursuant to this Agreement.

2.5. Hospital/Doctor agrees to maintain a record of all disclosures of Protected Health Information, including disclosures not made for the purposes of this Agreement, and further agrees within ten (10) days of a written request from HB Computers, to provide to HB Computers such information as is necessary to permit HB Computers to respond to a request by an individual for an accounting of the disclosures of the individual's Protected Health Information in accordance with 45 C.F.R. § 164.528. Hospital/Doctor further agrees to comply with the requirements of HITECH to provide HB Computers with an accounting of all disclosures made for treatment, payment and health care operations when the HITECH statute requiring such an accounting becomes applicable to HB Computers. HB Computers agrees to notify Hospital/Doctor in advance of the applicability of this requirement.

2.6. Hospital/Doctor agrees to report to HB Computers any unauthorized use or disclosure of Protected Health Information by Hospital/Doctor or its workforce, agents or subcontractors and the remedial action taken or proposed to be taken with respect to such use or disclosure in accordance with the specific provisions of Section 2.11.

2.7 Hospital/Doctor agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from HB Computers, or created or received by Hospital/Doctor on behalf of HB Computers, available to the Secretary of the United States Department of Health and Human Services, for purposes of determining HB Computers' compliance with HIPAA.

2.8. Within thirty (30) days of a written request, Hospital/Doctor shall allow a person who is the subject of Protected Health Information, such person's legal representative, or HB Computers to have access to and to copy such person's Protected Health Information maintained by Hospital/Doctor. Hospital/Doctor shall provide Protected Health Information in the format requested by such person, legal representative, or practitioner unless it is not readily producible in such format, in which case it shall be produced in standard hard copy format. Hospital/Doctor acknowledges that HITECH requires HB Computers and Hospital/Doctor to provide electronic health records to the individual in electronic format, and Hospital/Doctor agrees that to the extent applicable, Hospital/Doctor will produce any Protected Health Information in electronic format in a manner requested by HB Computers or by the individual who has made the request.

2.9 Within ten (10) days of a written request by HB Computers, Hospital/Doctor shall make available to HB Computers Protected Health Information received from or on behalf of HB Computers for amendment in accordance with 45 C.F.R. § 164.526. Hospital/Doctor further agrees to make such amendment to Protected Health Information as directed by HB Computers within thirty (30) days of a written request by HB Computers.

2.10 Hospital/Doctor shall implement and document appropriate administrative, physical and technical safeguards to preserve the confidentiality, integrity, and availability of all Protected Health Information and to prevent any unauthorized use or disclosure of Protected Health Information, or any breach or security incident, or other material breach or violation of an underlying contract, this Agreement, HIPAA and HITECH involving said Protected Health Information. Hospital/Doctor shall further:

2.10.1 Establish administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by § 164.314 of the Security Regulations. Hospital/Doctor represents and warrants that its security program is periodically reviewed and appropriate updates are implemented to address any gaps identified in its security program.

Hospital/Doctor agrees to make its security policies and procedures available to HB Computers upon reasonable request.

2.10.2 Require all its subcontractors and agents that receive, use or have access to Protected Health Information to implement reasonable and appropriate security safeguards to protect it from unauthorized use or disclosure, and to report any improper use or disclosure of Protected Health Information in the time and manner required by Hospital/Doctor herein.

2.10.3 Immediately report to HB Computers any unauthorized or improper use or disclosure of Protected Health Information, including without limitation, any security or privacy incident or breach involving the Protected Health Information (“Incident”) without unreasonable delay, and not more than twenty-four (24) hours after Business

Associate becomes aware of the Incident by Hospital/Doctor or its workforce, agents or subcontractors, and to provide HB Computers with notice and a report containing all information necessary to permit HB Computers to timely comply with HIPAA notification provisions and its implementing rules or any other applicable reporting law, if necessary. Said report shall identify:

(i) the known facts and circumstances related to the Incident;

(ii) the individuals affected;

(iii) the Protected Health Information that is known to be the subject of the Incident; (iv) the persons who are known to have information about the Incident; and (v) the corrective action that Hospital/Doctor took or will take to mitigate any deleterious effects of the Incident and to prevent future incidents.

Hospital/Doctor further acknowledges that it is familiar with the requirements of I.C. 4-1-11 concerning breaches of security and notification of disclosures of social security numbers. To the extent Hospital/Doctor must make its own notification involving any disclosure of Protected Health Information, Hospital/Doctor agrees to cooperate with HB Computers regarding the notification process before making such notification.

2.10.4 Implement reasonable policies and procedures designed to detect and provide appropriate response to relevant “Red Flags” that identity theft may be occurring (as defined in 16 CFR 681.2) or that may arise in the performance of Hospital/Doctor’s activities, if

Hospital/Doctor has access to information protected under the Red Flag Rules. Hospital/Doctor agrees that policies and procedures to detect relevant “Red Flags” are updated periodically. Hospital/Doctor further agrees to notify HB Computers of the detection of a Red Flag and to implement reasonable steps to prevent or mitigate identity theft.

### **3. TERM AND TERMINATION**

3.1 This Agreement shall commence as of the date first signed below, and the obligations set forth in this Agreement shall continue in effect if Hospital/Doctor uses, discloses, creates, receives or otherwise possesses any Protected Health Information created or received from or on behalf of HB Computers and until all such Protected Health Information is destroyed or returned to HB Computers pursuant to the terms of this Agreement.

3.2 HB Computers may immediately terminate this Agreement and the Primary Agreement if HB Computers determines that the Hospital/Doctor has breached a material term of this Agreement. Alternatively, HB Computers may choose to: (i) provide Business

Associate an opportunity to cure said alleged material breach to the satisfaction of HB Computers within ten (10) days. The Hospital/Doctor’s failure to cure shall be grounds for immediate termination of this Agreement. HB Computers’ remedies under this Agreement are cumulative, and the exercise of any remedy shall not preclude the exercise of any other.

3.3. Upon termination of this Agreement, Hospital/Doctor shall return or destroy, by rendering the Protected Health Information unusable, unreadable or undecipherable or beyond the ability to recover, all Protected Health Information received from HB Computers, or created or received by Hospital/Doctor on behalf of HB Computers and that Hospital/Doctor maintains in any form, and Hospital/Doctor shall retain no copies of such information. If the parties mutually agree that return or destruction of Protected Health Information is not feasible, Hospital/Doctor shall continue to maintain the security and privacy of such Protected Health Information in a manner consistent with the obligations of this Agreement and as required by California state law, and shall limit further use of the information to those purposes that make the return or destruction of the information infeasible. The duties hereunder to maintain the security and privacy of Protected Health Information shall survive the termination of this Agreement

### **4. AMENDMENT TO AGREEMENT**

HB Computers may amend this Agreement by providing ten (10) days prior written notice to Hospital/Doctor to maintain compliance with California or Federal laws or regulations. Such amendment shall be binding upon Hospital/Doctor at the end of the ten (10) day period and shall not require the consent of Hospital/Doctor. Hospital/Doctor may elect to terminate the Agreement within the ten (10) day period, but Hospital/Doctor’s obligations to maintain the security and privacy of Protected Health Information as required herein shall survive such termination. HB Computers and Hospital/Doctor may otherwise amend this Agreement by mutual written agreement.

## 5. INDEMNITY

Hospital/Doctor shall, to the fullest extent permitted by law, protect, defend, indemnify and hold harmless HB Computers and his/her respective employees, directors, and agents (“Indemnitees”) from and against any and all losses, costs, claims, penalties, fines, demands, liabilities, legal actions, judgments, and expenses of every kind (including reasonable attorney’s fees, including at trial and on appeal) asserted or imposed against any Indemnitees arising out of the acts or omissions of Hospital/Doctor or any subcontractor of or consultant of Hospital/Doctor or any of Hospital/Doctor's employees, directors, or agents related to the performance or nonperformance of this Agreement.

## 6. NO THIRD-PARTY BENEFICIARIES

Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or permitted assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

## 7. LIMITATION OF LIABILITY

NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND OR NATURE, WHETHER SUCH LIABILITY IS ASSERTED BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

## 8. DEFINITIONS

8.1 Limited Data Set. “Limited Data Set” shall have the meaning set out in 45 C.F.R. § 164.514(e)(2), as amended from time to time.

8.2 Protected Health Information. “Protected Health Information” shall have the meaning set out in 45 C.F.R. §160.103, as amended or revised from time to time. The term shall also include any social security numbers provided or made available to Hospital/Doctor.

45 Required by Law. “Required by Law” shall have the meaning set forth in C.F.R. §164.103, as amended or revised from time to time.

**HB COMPUTERS**

**HOSPITAL/DOCTOR**

By: \_\_\_\_\_

By: \_\_\_\_\_

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Print Title

\_\_\_\_\_  
Print Title

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date