HHSC BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT ("Agreement") is made by and between Hawaii Health Systems Corporation, a public body corporate and politic and an instrumentality and agency of the State of Hawaii ("HOSPITAL" or "HHSC"), and **Insert Name of Vendor** (hereinafter "BUSINESS ASSOCIATE"), a **Fill in type of business--e.g. sole proprietor, professional corporation or LLC** under the laws of the State of **Fill in Name of State**, whose business address is as follows: **Insert Street Address, Insert City**, **Insert State, Insert Zip Code**. **HHSC and BUSINESS ASSOCIATE are sometimes collectively hereinafter referred to as the "Parties", each a "Party".**

RECITALS

A. HHSC is a Covered Entity under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Title XIII of Division A, and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, and its implementing regulations at 45 C.F.R. Parts 160, 162 and 164 (the "HIPAA Rules").

B. BUSINESS ASSOCIATE agreed to provide the purchased product or service described in the underlying contract attached hereto as Exhibit A and made a part hereof ("Contract"), to perform its obligations under the Contract, or in furtherance of its business relationship with HHSC as described in the Contract, as applicable.

C. The Parties have determined that BUSINESS ASSOCIATE is deemed a "business associate" of HHSC, as defined by the HIPAA Rules, and wish to memorialize their respective obligations under pertinent laws and regulations.

NOW, THEREFORE, in consideration of the recitals above and the mutual covenants and conditions contained herein, HOSPITAL and BUSINESS ASSOCIATE agree as follows:

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

1. **BUSINESS ASSOCIATE'S OBLIGATIONS**.

BUSINESS ASSOCIATE agrees to:

a. Not use or disclose PHI other than as permitted or required by the Agreement or as Required By Law. In no event may BUSINESS ASSOCIATE use or further disclose PHI in a manner that would violate HIPAA if done by HHSC.

b. Not use PHI to create de-identified information for purposes unrelated to the Contract without HHSC's advance written approval. BUSINESS ASSOCIATE will use and request only the minimum PHI necessary to accomplish the permissible purpose of the use or request and shall comply with the minimum necessary standard under 45 C.F.R. § 164.502(b), as amended from time to time.

c. Implement appropriate safeguards, and comply, where applicable, with the Security Rule to ensure the confidentiality, integrity, and availability of all PHI BUSINESS ASSOCIATE creates, receives, maintains, or transmits on behalf of HHSC; protect against any reasonably anticipated threats or hazards to the security or integrity of PHI; prevent use or disclosure of PHI other than as provided for by this Agreement or as Required by Law; and ensure compliance with the HIPAA Rules by BUSINESS ASSOCIATE's Workforce. These safeguards include, but are not limited to:

(i) Administrative Safeguards. BUSINESS ASSOCIATE shall implement policies and procedures to prevent, detect, contain, and correct security violations, and reasonably preserve and protect the confidentiality, integrity, and availability of PHI (which includes EPHI), as required by 45 C.F.R. § 164.308, and enforcing those policies and procedures, including sanctions for anyone not found in compliance;

(ii) Technical and Physical Safeguards. BUSINESS ASSOCIATE shall implement appropriate technical safeguards, as required by 45 C.F.R. §§ 164.310 and 164.312, to protect PHI, including access controls, authentication, and transmission security, as well as implement appropriate physical safeguards to protect PHI, including workstation security and device and media controls; and

(iii) Training. BUSINESS ASSOCIATE shall provide training to its relevant Workforce members, including its management employees, on how to prevent the improper access, use or disclosure of PHI; and update and repeat training on a regular basis. For purposes of this Agreement, "relevant Workforce members" means BUSINESS ASSOCIATE's employees, volunteers, trainees, and other persons whose conduct, in the performance of work for BUSINESS ASSOCIATE: (1) is under the direct control of the BUSINESS ASSOCIATE, whether they are paid by BUSINESS ASSOCIATE and (2) involves direct access to PHI.

d. Within ten (10) days of signing this Agreement, BUSINESS ASSOCIATE shall provide HHSC with a list of individual employees and subcontractors who will require access to HHSC's electronic and computer systems to perform duties pursuant to the Contract. BUSINESS ASSOCIATE shall require all such persons to execute additional confidentiality documentation, as may be required by HHSC, prior to receiving such access. If any such person terminates employment or contract status with BUSINESS ASSOCIATE or its subcontractors, BUSINESS ASSOCIATE shall notify HHSC in writing no later than **five (5) business days** in advance of same, or in any event immediately upon termination, so that HHSC may terminate the individual's access to HHSC's systems.

e. In accordance with 45 C.F.R. § 164.316, document the required policies and procedures and keep them current, and shall cooperate in good faith in response to any reasonable requests from HHSC to discuss, review, inspect, and/or audit BUSINESS ASSOCIATE's safeguards. BUSINESS ASSOCIATE shall retain the documentation required for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

f. Acknowledge and agree that any and all PHI that BUSINESS ASSOCIATE creates, receives, maintains, or transmits shall not be accessed, generated, hosted, downloaded, printed, stored, processed, transferred, or maintained outside of the United States by BUSINESS ASSOCIATE or its subcontractor(s) without HHSC's prior written approval.

g. Not directly or indirectly pay or receive remuneration in exchange for PHI or otherwise engage in the sale of PHI in a manner that would be impermissible for BUSINESS ASSOCIATE under HIPAA or would be impermissible if done by HHSC under HIPAA.

h. Ensure that any subcontractor of BUSINESS ASSOCIATE that creates, receives, maintains, or transmits PHI on behalf of BUSINESS ASSOCIATE agrees in writing to the same restrictions, conditions and requirements that apply to BUSINESS ASSOCIATE through this Agreement with respect to such PHI.

i. Notify HHSC following discovery of any use or disclosure of PHI not permitted by this Agreement of which it becomes aware, or any Breach of Unsecured PHI.
   (i) BUSINESS ASSOCIATE shall immediately notify HHSC verbally or by telephone within 24 hours of its discovery or disclosure in violation of this Agreement.
   (ii) BUSINESS ASSOCIATE shall subsequently notify HHSC in writing, without unreasonable delay, and in no case later than two (2) business days following discovery of the impermissible use or disclosure of PHI, or Breach of Unsecured PHI.
   (iii) A Breach of Unsecured PHI shall be treated as discovered by the BUSINESS ASSOCIATE as of the first day on which such breach is known to the BUSINESS ASSOCIATE or, by exercising reasonable diligence, would have been known to the BUSINESS ASSOCIATE. BUSINESS ASSOCIATE shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the BUSINESS ASSOCIATE.

j. Take prompt (but in any event not more than two (2) business days) corrective action to mitigate, to the extent practicable, any harmful effect that is known to BUSINESS ASSOCIATE of a Security Incident or a misuse or unauthorized disclosure of PHI by BUSINESS ASSOCIATE in violation of this Agreement, and any other action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations. BUSINESS ASSOCIATE shall reasonably cooperate with HHSC's efforts to seek appropriate injunctive relief or otherwise prevent or curtail potential or actual Breaches, or to recover its PHI, including complying with a reasonable corrective action plan.

k. Investigate such Breach and provide to HHSC a written report of BUSINESS ASSOCIATE'S investigation and resultant mitigation within fifteen (15) calendar days of the discovery of the Breach.

l. Provide the following information with respect to a Breach of Unsecured PHI, to the extent possible, as the information becomes available, to HHSC's HIPAA Privacy and/or Security Officer:
   (i) 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
   (ii) Any other available information that HHSC is required to include in notification to the Individual under the HIPAA Rules, including, but not limited to the following:
      A. Contact information for Individuals who were or who may have been impacted by the Breach (e.g., first and last name, mailing address, street address, phone number, and email address);
      B. A brief description of the circumstances of the Breach, including the date of the Breach and date of discovery, if known;
      C. A description of the types of Unsecured PHI involved in the Breach (such as whether the full name, social security number, date of birth, address, account number, diagnosis, diagnostic, disability or billing codes, or similar information was involved);
      D. A brief description of what the BUSINESS ASSOCIATE has done or is doing to investigate the Breach, mitigate harm to the Individual(s) impacted by the Breach, and protect against future Breaches; and
      E. Contact information for BUSINESS ASSOCIATE's liaison responsible for investigating the Breach and communicating information relating to the Breach to HHSC.

m. Promptly report (but in any event not more than two (2) business days) to HHSC any Security Incident of which BUSINESS ASSOCIATE becomes aware with respect to EPHI that is in the custody of BUSINESS ASSOCIATE, including breaches of Unsecured PHI as required by 45 C.F.R. § 164.410, by contacting HHSC's HIPAA Privacy and/or Security Officer.

n. Implement reasonable and appropriate measures to ensure compliance with the requirements of this Agreement by Workforce members who assist in the performance of functions or activities on behalf of HHSC under this Agreement and use or disclose PHI, and discipline such Workforce members who intentionally violate any provisions of these special conditions, which may include termination of employment.

o. Make its internal policies, procedures, books and records relating to the use and disclosure of PHI received from, or created or received by BUSINESS ASSOCIATE on behalf of, HHSC available to the Secretary or to HHSC if necessary or required to assess BUSINESS ASSOCIATE's or HHSC's compliance with the HIPAA Rules. BUSINESS ASSOCIATE shall promptly notify HHSC of communications with the U.S. Department of Health and Human Services ("HHS") regarding PHI provided by or created by HHSC and shall provide HHSC with copies of any information BUSINESS ASSOCIATE has made available to HHS under this Section.

p. Upon notice from HHSC, accommodate any restriction to the use or disclosure of PHI and any request for confidential communications to which HHSC has agreed in accordance with the Privacy Rule.

q. Make available PHI held by BUSINESS ASSOCIATE, which HHSC has determined to be part of its Designated Record Set, within five (5) days to HHSC as necessary to satisfy HHSC's

obligations to provide an Individual with access to PHI under 45 C.F.R. § 164.524, as amended from time to time, in the manner designated by HHSC. In the event any individual requests access to PHI directly from BUSINESS ASSOCIATE, BUSINESS ASSOCIATE shall within two (2) days forward such request to HHSC. Any decision to deny access to PHI requested by an individual shall be made only by HHSC.

r. Make available PHI held by BUSINESS ASSOCIATE, which HHSC has determined to be part of its Designated Record Set, for amendment and incorporate any such amendments to PHI that HHSC directs or agrees to in accordance with 45 C.F.R. § 164.526, as amended from time to time, within five (5) days receipt of a request from HHSC or an Individual.

s. Document disclosures of PHI made by BUSINESS ASSOCIATE, which are required to be accounted for under 45 C.F.R. § 164.528(a)(1), and within ten (10) days of notice by HHSC to BUSINESS ASSOCIATE that HHSC has received a request for an accounting of disclosures of PHI regarding an Individual made during a period of time less than six (6) years prior to the date on which the accounting was requested, BUSINESS ASSOCIATE shall make available to HHSC such information as is in BUSINESS ASSOCIATE's possession and is required for HHSC to make the accounting required by 45 C.F.R. § 164.528, as amended from time to time. At a minimum, BUSINESS ASSOCIATE shall provide HHSC with the following information: (1) the date of the disclosure; (2) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (3) a brief description of the PHI disclosed; and (4) 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 of receipt forward such request to HHSC. It shall be the responsibility of HHSC to prepare and deliver any such accounting requested. BUSINESS ASSOCIATE hereby agrees to implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section.

2. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.

BUSINESS ASSOCIATE may, except as otherwise limited in this Agreement:

a. General Use and Disclosure: Create, receive, maintain or transmit PHI to provide the purchased product or service described in the Contract, to perform its obligations under the Contract, or in furtherance of its business relationship with HHSC as described in the Contract, as applicable and this Agreement, provided that the use or disclosure would not violate the HIPAA Rules if done by HHSC.

b. Limited Use of PHI for BUSINESS ASSOCIATE’s Benefit. Use PHI received by the BUSINESS ASSOCIATE in its capacity as HHSC’s BUSINESS ASSOCIATE, if necessary, for the proper management and administration of BUSINESS ASSOCIATE or to carry out the legal responsibilities of BUSINESS ASSOCIATE. BUSINESS ASSOCIATE’s proper management and administration does not include the use or disclosure of PHI by BUSINESS ASSOCIATE for marketing purposes or for sale of PHI.

c. Limited Disclosure of PHI for BUSINESS ASSOCIATE’s Benefit. Disclose PHI for BUSINESS ASSOCIATE’s proper management and administration or to carry out its legal responsibilities only if the disclosure is Required By Law, or BUSINESS ASSOCIATE obtains reasonable written assurances from the person or entity to whom PHI is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for

which it was disclosed to the person or entity, and the person notifies BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of PHI has been breached.

d. Minimum Necessary. BUSINESS ASSOCIATE shall only request, use, and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure.

e. Data Aggregation. Use PHI to provide Data Aggregation services relating to HHSC's Health Care Operations as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B), as may be amended from time to time.

f. Disclosures by Whistleblowers: Use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1), as may be amended from time to time.

3. HHSC'S OBLIGATIONS.

a. HHSC shall not request BUSINESS ASSOCIATE to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by HHSC.

b. HHSC shall not provide BUSINESS ASSOCIATE with more PHI than is minimally necessary for BUSINESS ASSOCIATE to perform its obligations as described in the Contract only in accordance with the HIPAA Rules.

4. TERM AND TERMINATION.

a. This Agreement shall be effective as of the date of the Contract, and shall continue in effect until terminated as provided in Section 4.b or until all of the PHI provided by HHSC to BUSINESS ASSOCIATE, or created or received by BUSINESS ASSOCIATE on behalf of HHSC, is destroyed or returned to HHSC.

b. Termination for Cause. In the event HHSC determines that BUSINESS ASSOCIATE has committed a material breach of this Agreement, HHSC may, in its discretion, either: (i) provide an opportunity for BUSINESS ASSOCIATE to cure the breach or end the violation, provided that HHSC may immediately terminate the Contract that requires the use of PHI if BUSINESS ASSOCIATE does not cure the breach or end the violation within the time frame specified by HHSC; or (ii) immediately terminate the Contract that requires the use of PHI if BUSINESS ASSOCIATE has breached a material term of this Agreement and HHSC determines in its sole discretion that a cure is not possible.

c. Effect of Termination.

(i) Upon termination of this Agreement, until notified otherwise by HHSC, BUSINESS ASSOCIATE shall extend all protections, limitations, requirements and other provisions of this Agreement to all PHI received from or on behalf of HHSC or created or received by BUSINESS ASSOCIATE on behalf of HHSC.

(ii) Except as otherwise provided in subsection 4(c)(iii) below, upon termination of this Agreement for any reason, BUSINESS ASSOCIATE shall, at HHSC's option, return or destroy all PHI received from HHSC, or created or received by the BUSINESS ASSOCIATE

on behalf of, HHSC that the BUSINESS ASSOCIATE still maintains in any form, and BUSINESS ASSOCIATE shall retain no copies of the information. This provision shall also apply to PHI that is in the possession of subcontractors or agents of BUSINESS ASSOCIATE. BUSINESS ASSOCIATE shall notify HHSC in writing of any and all conditions that make return or destruction of such information not feasible and shall provide HHSC with any requested information related to HHSC's determination as to whether the return or destruction of such information is feasible.

(iii) If HHSC determines that returning or destroying any or all PHI is not feasible or opts not to require the return or destruction of such information, the protections of this Agreement shall continue to apply to such PHI, and BUSINESS ASSOCIATE shall limit further uses and disclosures of PHI to those purposes that make the return or destruction infeasible, for so long as BUSINESS ASSOCIATE maintains such PHI. HHSC hereby acknowledges and agrees that infeasibility includes BUSINESS ASSOCIATE's need to retain PHI for purposes of complying with its work product documentation standards.

5. MISCELLANEOUS.

a. Amendment. BUSINESS ASSOCIATE and HHSC agree to take such action as is necessary to amend this Agreement from time to time for compliance with the requirements of the HIPAA Rules and any other applicable law.

b. Interpretation. In the event that any terms of this Agreement are inconsistent with the terms of the Contract, then the terms of this Agreement shall control. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Rules, as amended, the HIPAA Rules shall control. Where provisions of this Agreement are different than those mandated in the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of this Agreement shall control. Any ambiguity in this Agreement shall be resolved to permit HHSC to comply with the HIPAA Rules. Notwithstanding the foregoing, nothing in this Agreement shall be interpreted to supersede any federal or state law or regulation related to confidentiality of health information that is more stringent than the HIPAA Rules.

c. Indemnification. BUSINESS ASSOCIATE shall defend, indemnify, and hold harmless HHSC and HHSC's directors, officers, employees, agents, contractors and subcontractors to the extent required under the Contract for incidents that are caused by or arise out of a Breach or failure to comply with any provision of this Agreement or the HIPAA Rules by BUSINESS ASSOCIATE or any of BUSINESS ASSOCIATE's officers, employees, agents, contractors or subcontractors.

d. Costs Related to Breach. BUSINESS ASSOCIATE shall be responsible for any and all costs incurred by HHSC as a result of any Breach of PHI by BUSINESS ASSOCIATE, its officers, directors, employees, contractors or agents, or by a third party to which the BUSINESS ASSOCIATE disclosed PHI under this Agreement, including but not limited to notification of individuals or their representatives of a Breach of Unsecured PHI, and the cost of mitigating any harmful effect of the Breach.

e. Response to Subpoenas. In the event BUSINESS ASSOCIATE receives a subpoena or similar notice or request from any judicial, administrative or other party which would require the production of PHI received from, or created for, HHSC, BUSINESS ASSOCIATE shall promptly,

in any event not more than two (2) days, forward a copy of such subpoena, notice or request to HHSC to afford HHSC the opportunity to timely respond to the demand for its PHI as HHSC determines appropriate according to its federal and state obligations.

f. Survival. The respective rights and obligations of HHSC and BUSINESS ASSOCIATE under Sections 4.c., Term and Termination, 5.c., Indemnification, and 5.d., Costs Related to Breach, shall survive the termination of this Agreement.

g. Notices: Whenever written notice is required by one Party to the other under this Agreement, it should be mailed, faxed or e-mailed, or any of the foregoing, to the appropriate address noted below. If notice is sent by e-mail, then a confirming written notice should be sent by mail or fax, or both, within two (2) business days after the date of the e-mail. The sender of any written notice required under this Agreement is responsible for confirming receipt by the recipient.

HHSC	**BUSINESS ASSOCIATE**
HIPAA Privacy Officer	
3675 Kilauea Avenue	
Honolulu, Hawaii 96816	
Phone: (808) 733-8430	
Fax: (808) 733-4167	
Email: privacyofficer@hhsc.org	

6. DEFINITIONS FOR USE IN THIS AGREEMENT.

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule, Breach Notification Rule, or the Security Rule.

"Breach Notification Rule" shall mean the Breach Notification of Unsecured Protected Health Information Rule, 45 C.F.R. Part 164, Subparts A and D, as amended from time to time.

"Designated Record Set" shall mean a group of records maintained by or for HHSC that is (1) the medical records and billing records about individuals maintained by or for HHSC, (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for HHSC to make decisions about individuals. As used herein, the term "Record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for HHSC.

"Electronic Media" shall mean the mode of electronic transmissions. It includes the Internet, extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

"Individually Identifiable Health Information" shall mean information that is a subset of health information, including demographic information collected from an individual, and:

(1) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

(2) relates to the past, present, or future physical or mental health or condition of an

individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and

(a) that identifies the individual, or

(b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Privacy Rule" shall mean the Standard for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and E, as amended from time to time.

"Protected Health Information" (or "PHI") shall mean Individually Identifiable Health Information that is (1) transmitted by electronic media; (2) maintained in any medium constituting electronic media; or (3) transmitted or maintained in any other form or medium. "PHI" shall not include: education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; records described in 20 U.S.C. § 1232g (a)(4)(B)(iv); employer records; or information about an individual who has been deceased for more than 50 years.

"Secretary" shall mean the Secretary of the United States Department of Health and Human Services.

"Security Incident" shall mean any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

"Security Rule" shall mean the Security Standard for electronic Protected Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and C, as amended from time to time.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

HHSC BUSINESS ASSOCIATE AGREEMENT

HOSPITAL/HHSC

Signature: _____

Name: _____

Title: _____

Date: _____

I hereby represent and warrant that I have the legal right and authority to execute this Agreement on behalf of the BUSINESS ASSOCIATE above named.

Business Associate

Signature: _____

Name: _____

Title: _____

Date: _____