

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”) is entered into by and between _____ (“Business Associate”), whose business address is _____, and the University of Hawai’i, the state university and a body corporate of the State of Hawai’i, whose business address is Bachman Hall, 2444 Dole Street, Honolulu, Hawai’i 96822, as a Hybrid Entity (hereinafter referred to as the “University” or the “Hybrid Entity”) pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended by the American Recovery and Reinvestment Act of 2009, which included the Health Information Technology for Economic and Clinical Health Act that expanded the scope of privacy and security protections, and by the implementing regulations at 45 Code of Federal Regulations (“CFR”) Parts 160, 162 and 164, as amended (collectively referred to as “HIPAA”). The [Insert UH COVERED COMPONENT Name] is a Health Care Component of the Hybrid Entity, is the Covered Entity under this Agreement, and will be referred to hereinafter as the “Covered Entity.” The Contractor signing this Agreement has signed a separate contract for services referred to as the “Contract” and will be referred to hereinafter as the “Business Associate.”

Business Associate will provide to Covered Entity certain services described in the Contract to which this Agreement is attached, and may have access to Protected Health Information (“PHI”), including electronic Protected Health Information (“ePHI”) (as such terms are defined below) in fulfilling its responsibilities under the Contract. To the extent Business Associate needs to create, receive, maintain, or transmit PHI to perform services under the Contract, it will be acting in the capacity of a Business Associate as defined in 45 CFR §160.103 of the Covered Entity and will be subject to the terms of this Agreement.

In consideration of Covered Entity's and Business Associate's continuing obligations under the Contract, and the mutual agreements below, the parties agree as follows:

I. DEFINITIONS

Except for terms otherwise defined herein, and unless the context indicates otherwise, capitalized terms used in this Agreement and the terms “person,” “use,” and “disclosure” are defined by the HIPAA regulations at 45 CFR Parts 160, 162, and 164, as amended (the “HIPAA Rules”). A change to the HIPAA Rules that modifies any defined term, or which alters the regulatory citation for the definition, shall be deemed to amend this Agreement.

- A. Breach: the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule (as defined below) or as provided for by this Agreement, which compromises the security or privacy of the PHI, 45 CFR §164.402.

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

1. An acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach unless the Business Associate demonstrates to the Covered Entity's satisfaction that there is a low probability that the PHI has been compromised based on a risk assessment that identifies at least the following: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.
 2. Breach excludes:
 - a. Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under the authority of the Business Associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
 - b. Any inadvertent disclosure by a person who is authorized to access PHI at the Business Associate to another person authorized to access PHI at the same Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
 - c. A disclosure of PHI where the Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- B. Designated Record Set: records, including but not limited to PHI maintained, collected, used, or disseminated by or for the Covered Entity relating to (i) medical and billing records about Individuals maintained by or for a covered Health Care Provider, (ii) enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for a Health Plan, or (iii) that are used in whole or in part by the Covered Entity to make decisions about Individuals, 45 CFR §164.501.
- C. Electronic Protected Health Information ("ePHI"): Information that is transmitted or maintained by electronic media that comes within the definition of PHI as defined below, 45 CFR §160.103.
- D. HIPAA Rules: the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and Part 164.
- E. Individual: the person who is the subject of PHI, and shall include a person who qualifies as a personal representative under 45 CFR §160.103.

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

- F. Personal Representative: Someone with the legal authority to act on behalf of an incompetent adult patient, a minor patient or a deceased patient or the patient's estate in making health care decisions or in exercising the patient's rights related to the individual's PHI, 45 CFR §164.502(g).
- G. Privacy Rule: the HIPAA Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160, and part 164, subparts A and E.
- H. Protected Health Information ("PHI"): any oral, paper or electronic information, data, documentation, and materials, including, but not limited to, demographic, medical, genetic and financial information that is created or received by a Health Care Provider, Health Plan, Employer, or Health Care Clearinghouse, and relates to the past, present, or future physical or mental health or 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 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. For purposes of this Agreement, the term Protected Health Information or PHI is limited to the information created, maintained, received, or transmitted by Business Associate on behalf of or from the Covered Entity under the Contract. PHI includes without limitation ePHI, and excludes education records under 20 U.S.C. §1232(g), employment records held by the Covered Entity as an employer, and records regarding an Individual who has been deceased for more than 50 years, 45 CFR §160.103.
- I. Security Rule: the HIPAA Security Standards for the Protection of Electronic Protected Health Information at 45 CFR part 160, and part 164, subparts A and C.
- J. Unsecured Protected Health Information or Unsecured PHI: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary under section 13402(h)(2) of Public Law 111-5, 45 CFR §164.402.

II. BUSINESS ASSOCIATE'S OBLIGATIONS

Business Associate agrees to:

- A. No unpermitted PHI use or disclosure. Not use or disclose PHI other than as permitted or required by this Agreement or as Required By Law. In no event may Business Associate use or further disclose PHI in a manner that would violate the Privacy Rule if done by the Covered Entity, except as expressly provided in this Agreement, 45 CFR §§164.502(a)(3), 164.504(e)(2)(ii)(A).
- B. Implement appropriate safeguards. Implement appropriate safeguards, and comply, where applicable, with the Security Rule to ensure the confidentiality,

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

integrity, and availability of all ePHI the Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity; protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI; 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, 45 CFR §164.306(a). These safeguards include, but are not limited to:

1. 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 ePHI, as required by 45 CFR §164.308, and enforce those policies and procedures, including sanctions for anyone not found in compliance, 45 CFR §164.308;
 2. Technical and Physical Safeguards. Business Associate shall implement appropriate technical safeguards 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, 45 CFR §§ 164.310, 164.312; and
 3. Training. Business Associate shall provide training to relevant workforce members, including management, on how to prevent the improper access, use or disclosure of PHI; and update and repeat training on a regular basis, 45 CFR §164.308(a)(5).
- C. Document and keep current required policies and procedures. In accordance with 45 CFR §164.316, document the required policies and procedures and keep them current, and cooperate in good faith in response to any reasonable requests from Covered Entity 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, 45 CFR §§164.306 - 164.316; 164.504(e)(2)(ii)(B).
- D. Business Associate subcontractors required to comply with Agreement. 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, 45 CFR §§164.308(b), 164.314(a)(2), 164.502(e), 164.504(e)(2)(ii)(D).
- E. Notify Covered Entity of any unpermitted PHI use or disclosure. Notify the Covered Entity 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, 45 CFR §§164.314(a)(2), 164.410(a), 164.504(e)(2)(ii)(C).

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

1. Immediate verbal notice to Covered Entity. Business Associate shall immediately notify the Covered Entity's University System HIPAA Privacy and Security Officer(s) and [UH COVERED COMPONENT's] Unit HIPAA Coordinator verbally.
 2. Prompt written notice to Covered Entity. Business Associate shall subsequently notify the Covered Entity's University System HIPAA Privacy and Security Officer(s) and [UH COVERED COMPONENT's] Unit HIPAA Coordinator in writing, without unreasonable delay, and in no case later than five (5) business days following discovery of the impermissible use or disclosure of PHI, or Breach of Unsecured PHI.
 3. Discovery date of Breach. 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 Business Associate or, by exercising reasonable diligence, would have been known to 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, official, or other agent of the Business Associate, 45 CFR §164.410(a)(2).
- F. Take prompt corrective action. Take prompt 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 the Covered Entity'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, 45 CFR §§ 164.308(a)(6); 164.530(f).
- G. Investigate Breach. Investigate such Breach and provide a written report of the investigation and resultant mitigation to Covered Entity's University System HIPAA Privacy and Security Officer(s) and [UH COVERED COMPONENT's] Unit HIPAA Coordinator within thirty (30) calendar days of the discovery of the Breach.
- H. Information to be provided with respect to a Breach. Provide the following information with respect to a Breach of Unsecured PHI, to the extent possible, as the information becomes available, to the Covered Entity's University System HIPAA Privacy and Security Officer(s) and [UH COVERED COMPONENT's] Unit HIPAA Coordinator:

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

1. Identification of individuals impacted by the Breach. 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
2. Include available information in notification to individual. Any other available information that the Covered Entity is required to include in notification to the Individual under the HIPAA Rules, including, but not limited to the following 45 CFR §§164.404(c)(l), 164.408, 164.410(c)(l) and (2):
 - a. Contact information for individuals impacted by the Breach. 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, and email address);
 - b. Describe circumstances of the Breach. A brief description of the circumstances of the Breach, including the date of the Breach and date of discovery, if known;
 - c. Description of PHI involved in Breach. 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 and/or billing codes, or similar information was involved);
 - d. Describe Business Associate investigation. 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. Business Associate liaison contact information. Contact information for Business Associate's liaison responsible for investigating the Breach and communicating information relating to the Breach to the Covered Entity.
- I. Promptly report Security Incident. Promptly report to Covered Entity's University System HIPAA Privacy and Security Officer(s) and [UH COVERED COMPONENT's] Unit HIPAA Coordinator 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 CFR §164.410, by contacting the University System HIPAA Privacy and Security Officer(s) and [UH COVERED COMPONENT's] Unit HIPAA Coordinator, 45 CFR §§164.314(a)(2), 164.410.

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

- J. Implement measures to ensure Agreement compliance. 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 the Covered Entity 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, 45 CFR §§164.308(a), 164.530(b) and (e).
- K. Make HIPAA policies and procedures available to HHS Secretary. 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, the Covered Entity available to the Secretary of Health and Human Services or to Covered Entity if necessary or required to assess Business Associate's or the Covered Entity's compliance with the HIPAA Rules. Business Associate shall promptly notify Covered Entity of communications with the U.S. Department of Health and Human Services (HHS) regarding PHI provided by or created by Covered Entity or Business Associate and shall provide Covered Entity with copies of any information Business Associate has made available to HHS under this paragraph, 45 CFR §164.504(e)(2)(ii)(I).
- L. Accommodate Covered Entity's restriction on use/disclosure. Upon notice from Covered Entity, accommodate any restriction to the use or disclosure of PHI and any request for confidential communications to which Covered Entity has agreed in accordance with the Privacy Rule, 45 CFR §164.522.
- M. Make PHI available to Covered Entity. Make available PHI held by Business Associate, which the Covered Entity has determined to be part of its Designated Record Set, to the Covered Entity as necessary to satisfy the Covered Entity's obligations to provide an Individual with access to the Individual's PHI under 45 CFR §164.524, in the time and manner designated by the Covered Entity, 45 CFR §§ 164.504(e)(2)(ii)(E), 164.524.
- N. Make PHI available for amendment. Make available PHI held by Business Associate, which the Covered Entity has determined to be part of its Designated Record Set, to amend any PHI that the Covered Entity directs or agrees to in accordance with 45 CFR §164.526, upon request of the Covered Entity or an Individual.
- O. Disclosure documentation. Document disclosures of PHI made by Business Associate, which are required to be accounted for under 45 CFR §164.528(a)(I), and make this information available as necessary to satisfy the Covered Entity's obligation to provide an accounting of disclosures to an Individual within five (5) business days by the Covered Entity of a request by an Individual of a request for an accounting of disclosures of PHI. If an

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

Individual directly requests an accounting of disclosures of PHI from Business Associate, Business Associate shall notify Covered Entity's University System HIPAA Privacy and Security Officer(s) and [UH COVERED COMPONENT's] Unit HIPAA Coordinator of the request within five (5) business days, and Covered Entity shall either direct Business Associate to provide the information directly to the Individual, or it shall direct that the information required for the accounting be forwarded to Covered Entity for compilation and distribution to the Individual, 45 CFR §§ 164.504(e)(2)(ii)(G) and (H), 164.528.

- P. Comply with HIPAA Rules. Comply with any other requirements of the HIPAA Rules not expressly specified in this Agreement, as and to the extent that such requirements apply to Business Associates under the HIPAA Rules, as the same may be amended from time to time.

III. 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 only for the purposes listed in the Contract and this Agreement, provided that the use or disclosure would not violate the HIPAA Rules if done by the Covered Entity or violate the Minimum Necessary requirements applicable to the Covered Entity, 45 CFR §§164.502(a) & (b), 164.504(e)(2)(i).
- B. Limited Use of PHI for Business Associate's Benefit. Use PHI received by the Business Associate in its capacity as the Covered Entity's Business Associate, if necessary, for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate to Covered Entity. 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, 45 CFR §§164.502(a)(5)(ii), 164.504(e)(2)(i)(A), 164.504(e)(4)(i), 164.508(a)(3) and (a)(4).

IV. TERM AND TERMINATION

- A. Commencement Date/Termination Date. This Agreement commences as of the date last signed on the signature page and shall remain in effect until terminated in accordance with the terms of this section, provided, however, that termination shall not affect the respective obligations or rights of the parties arising under this Agreement prior to the effective date of termination, all of which shall continue in accordance with their terms.
- B. Covered Entity may terminate Agreement. Covered Entity shall have the right to terminate this Agreement for any reason, including determination that

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

Business Associate has violated a material term of this Agreement, upon thirty (30) days written notice to Business Associate. Such termination of this Agreement shall simultaneously terminate the Contract on the same effective date, unless otherwise agreed to in writing by both parties. If a breach of this Agreement is determined to be willful or incurable by either party, then a party may give written notice of immediate termination of this Agreement.

- C. If Contract terminated, Agreement terminated. Upon the termination of the Contract, this Agreement will automatically terminate.
- D. Upon expiration or termination of Agreement, return all PHI to Covered Entity. Upon termination of this Agreement for any reason, Business Associate agrees either 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, unless return or destruction is not feasible or lawful, or unless other legal grounds exist for retaining the PHI. In the case of PHI which is not returned or destroyed, 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, or as otherwise permitted by law, 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, 45 CFR 164.504 (e)(2)(ii)(J).

V. NOTICES

Whenever written notice is required by one party to the other under this Agreement, written notice shall be delivered, mailed, or faxed to the address or fax number below. If notice is delivered, it is effective when received during normal business hours with a written proof of service saved for the record. If notice is mailed, it is effective no sooner than three (3) business days after it is mailed by either certified mail or registered mail. If notice is faxed, it is effective when the confirmation fax is printed.

[SIGNATURE PAGE FOLLOWS]

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

SIGNATURES EXECUTING THIS AGREEMENT: IN WITNESS WHEREOF, this Agreement has been executed by the authorized representative(s) of the Covered Entity and the authorized representative(s) of the Business Associate.

UNIVERSITY OF HAWAII COVERED ENTITY _____ Signature _____ Printed Name _____ Address of [UH COVERED COMPONENT] _____ Telephone no. of [UH COVERED COMPONENT] _____ Fax no. of [UH COVERED COMPONENT] _____ Mobile Phone No. of [Project Principal Investigator or Program Lead] _____ COVERED ENTITY _____ Date of execution	[Insert Business Associate Name] BUSINESS ASSOCIATE: _____ Signature of Project Principal Investigator or Program Lead _____ Printed Name _____ Address _____ Telephone no. _____ Fax no. _____ Mobile Phone No. _____ BUSINESS ASSOCIATE _____ Date of execution
_____ Signature of University System HIPAA Privacy Officer	
_____ Signature of Campus Chancellor (or designee) for campus projects, or appropriate System Vice President (or	

ATTACHMENT 3-A
UNIVERSITY BUSINESS ASSOCIATE AGREEMENT
(UNIT AS THE COVERED ENTITY)

designee) for System projects	
-------------------------------	--

END