

EXHIBIT A

SUBCONTRACTOR BUSINESS ASSOCIATE AGREEMENT

Under the Contract to which this Subcontractor Business Associate Agreement is attached (the Contract), the Benefits, Employment and Support Services Division of the Department of Human Services, State of Hawaii (BESSD) is a Business Associate¹ of the Department of Human Services, Med-QUEST Division (MQD), a Covered Entity under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), as amended, and its implementing regulations at 45 CFR parts 160 and 164 (the HIPAA Rules), and has entered into that certain Business Associate Memorandum of Agreement attached hereto as Attachment 1 (MQD-BESSD MOA).

CONTRACTOR will provide to BESSD certain services described in the Contract, and may have access to Protected Health Information (PHI) that BESSD creates, accesses, receives, maintains, or transmits from or on behalf of MQD in fulfilling its responsibilities under the Contract. To the extent CONTRACTOR needs to create, access, receive, maintain or transmit PHI to perform services under the Contract, it will be acting as a Subcontractor of BESSD as defined in the HIPAA Rules and is required to agree to the same terms that BESSD is subject to under the MQD-BESSD MOA. CONTRACTOR must comply with the HIPAA Rules and the terms of this Agreement and is, therefore, referred to as “BUSINESS ASSOCIATE” in this Agreement.

In consideration of BESSD’s and BUSINESS ASSOCIATE’s continuing obligations under the Contract, and the mutual agreements below, the parties agree as follows:

1. DEFINITIONS.

Except for terms otherwise defined herein, and unless the context indicates otherwise, any other capitalized terms used in this Agreement and the terms “person,” “use,” and “disclosure” are defined by 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 incorporated into this Agreement.

Breach² means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule or as provided for by this Agreement, which compromises the security or privacy of the PHI.

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 BESSD’s and MQD’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

¹ Business Associate is defined at 45 CFR §160.103

² Breach: 45 CFR §164.402.

made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.

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.

Designated Record Set means records, including but not limited to PHI maintained, collected, used, or disseminated by or for MQD 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 MQD to make decisions about Individuals.³

Electronic Protected Health Information (EPHI) means PHI that is transmitted by Electronic Media or maintained in Electronic Media.⁴

HIPAA Rules shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and Part 164, as amended.

Individual means the person who is the subject of Protected Health Information, and shall include a person who qualifies as a personal representative under 45 CFR §164.502(g) of the HIPAA Rules.⁵

Privacy Rule means the HIPAA Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160, and part 164, subparts A and E, as amended.

Protected Health Information (PHI) means 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

³ Designated Record Set: 45 CFR §164.501.

⁴ Electronic Protected Health Information: 45 CFR §160.103

⁵ Individual: 45 CFR §160.103; 164.502(g)

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 is limited to the information created, maintained, accessed, received, or transmitted by BUSINESS ASSOCIATE on behalf of or from BESSD or MQD under the Contract. Protected Health Information includes without limitation EPHI, and excludes education records under 20 U.S.C. §1232(g), employment records held by BESSD or MQD as an employer, and records regarding an Individual who has been deceased for more than 50 years.⁶

Security Rule means the HIPAA Security Standards for the Protection of Electronic Protected Health Information at 45 CFR part 160, and part 164, subpart C, as amended.

Unsecured Protected Health Information or Unsecured PHI means 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 111-5.⁷

2. BUSINESS ASSOCIATE'S OBLIGATIONS.

BUSINESS ASSOCIATE agrees to:

- a. Not use or disclose PHI other than as permitted or required by the Contract, this Agreement, the MQD-BESSD MOA, 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 BESSD or MQD, except as expressly provided in this Agreement.⁸
- b. Implement appropriate safeguards and comply with the Security Rule to ensure the confidentiality, integrity, and availability of all EPHI the BUSINESS ASSOCIATE creates, receives, maintains, or transmits on behalf of BESSD; 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.⁹ 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

⁶ Protected Health Information: 45 CFR §160.103

⁷ Unsecured Protected Health Information: 45 CFR §164.402

⁸ 45 CFR §§164.502(a)(3), 164.504(e)(2)(ii)(A)

⁹ 45 CFR §164.306(a)

EPHI, as required by 45 CFR §164.308, and enforcing those policies and procedures, including sanctions for anyone not found in compliance;¹⁰

- (ii) 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;¹¹ and
 - (iii) 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.¹²
- c. In accordance with 45 CFR §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 BESSD 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.¹³
 - d. 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.¹⁴ For purposes of this Agreement, a Subcontractor's breach of a Subcontractor Business Associate Agreement shall constitute a breach of this Agreement by BUSINESS ASSOCIATE.
 - e. Notify BESSD 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, including use or disclosure of PHI or Breach of Unsecured PHI by a Subcontractor.¹⁵
 - (i) BUSINESS ASSOCIATE shall immediately notify BESSD verbally.
 - (ii) BUSINESS ASSOCIATE shall subsequently notify BESSD in writing, without unreasonable delay, and in no case later than twenty-four (24) hours 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

¹⁰ 45 CFR §164.308

¹¹ 45 CFR §§ 164.310, 164.312

¹² 45 CFR §164.308(a)(5)

¹³ 45 CFR §§164.306 – 164.316; 164.504(e)(2)(ii)(B)

¹⁴ 45 CFR §§164.308(b), 164.314(a)(2), 164.502(e), 164.504(e)(2)(ii)(D)

¹⁵ 45 CFR §§164.314(a)(2), 164.410(a), 164.504(e)(2)(ii)(C)

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.¹⁶

- f. 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 BESSD's and MQD'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.¹⁷
- g. Investigate such Breach and provide a written report of the investigation and resultant mitigation to BESSD within thirty (30) calendar days of the discovery of the Breach.
- h. Provide the following information with respect to a Breach of Unsecured PHI, to the extent possible, as the information becomes available, to BESSD:
 - (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 MQD is required to include in notification to the Individual under the HIPAA Rules, including, but not limited to the following:¹⁸
 - A. 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. 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 and/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

¹⁶ 45 CFR §164.410(a)(2)

¹⁷ 45 CFR §§164.308(a)(6); 164.530(f)

¹⁸ 45 CFR §§164.404(c)(1), 164.408, 164.410(c)(1) and (2)

- E. Contact information for BUSINESS ASSOCIATE's liaison responsible for investigating the Breach and communicating information relating to the Breach to BESSD.
- i. Promptly report to BESSD 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 §164.410.¹⁹
 - j. 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 BESSD 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.²⁰
 - k. 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, BESSD available to the Secretary or to STATE if necessary or required to assess BUSINESS ASSOCIATE's or the STATE's compliance with the HIPAA Rules. BUSINESS ASSOCIATE shall promptly notify STATE of communications with the U.S. Department of Health and Human Services (HHS) regarding PHI provided by or created by STATE and shall provide STATE with copies of any information BUSINESS ASSOCIATE has made available to HHS under this paragraph.²¹
 - l. Upon notice from BESSD or MQD, accommodate any restriction to the use or disclosure of PHI and any request for confidential communications to which MQD has agreed in accordance with the Privacy Rule.²²
 - m. Make available PHI held by BUSINESS ASSOCIATE, which MQD has determined to be part of its Designated Record Set, to MQD as necessary to satisfy MQD's obligations to provide an Individual with access to PHI under 45 CFR §164.524, in the time and manner designated by MQD.²³
 - n. Make available PHI held by BUSINESS ASSOCIATE, which MQD has determined to be part of its Designated Record Set, for amendment and incorporate any amendments to PHI that MQD directs or agrees to in accordance with 45 CFR §164.526, upon request of MQD or an Individual.
 - o. Document disclosures of PHI made by BUSINESS ASSOCIATE, which are required to be accounted for under 45 CFR §164.528(a)(1), and make this information available as necessary to satisfy MQD's obligation to provide an accounting of disclosures to an Individual within two (2) business days' notice by MQD of a request by an Individual of a request for an accounting of disclosures of PHI. If an Individual directly requests an

¹⁹ 45 CFR §§164.314(a)(2), 164.410

²⁰ 45 CFR §§164.308(a), 164.530(b) and (e)

²¹ 45 CFR §504(e)(2)(ii)(I)

²² 45 CFR §164.522

²³ 45 CFR §§164.504(e)(2)(ii)(E), 164.524

accounting of disclosures of PHI from BUSINESS ASSOCIATE, BUSINESS ASSOCIATE shall notify BESSD and MQD of the request within two (2) business days, and MQD 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 MQD for compilation and distribution to the Individual.²⁴

- p. 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.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.

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

- a. General Use and Disclosure. Create, access, 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 BESSD or MQD or violate the Minimum Necessary requirements applicable to BESSD or MQD.²⁵
- b. Limited Use of PHI for BUSINESS ASSOCIATE's Benefit. Use PHI received by the BUSINESS ASSOCIATE in its capacity as the BESSD'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. 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.²⁶
- 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 assurances from the person 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, and the person notifies BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of PHI has been breached.²⁷
- d. Minimum Necessary. BUSINESS ASSOCIATE shall only request, access, use, and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure.²⁸
- e. Data Aggregation. Use PHI to provide Data Aggregation services relating to the MQD's Health Care Operations as permitted by 45 CFR §164.504(e)(2)(i)(B).

²⁴ 45 CFR §§164.504(e)(2)(ii)(G) and (H), 164.528; HAR ch. 2-71, subch. 2.

²⁵ 45 CFR §§164.502(a) & (b), 154.504(e)(2)(i)

²⁶ 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)

²⁷ 45 CFR §164.504(e)(4)(ii)

²⁸ 45 CFR §164.502(b)

- f. Disclosures by Whistleblower. Use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

4. STATE'S OBLIGATIONS.

- a. BESSD 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 BESSD.
- b. BESSD shall not provide BUSINESS ASSOCIATE with access to more PHI than is minimally necessary for BUSINESS ASSOCIATE to provide the services under the Contract and BESSD shall provide any PHI needed by BUSINESS ASSOCIATE to perform under the Contract only in accordance with the HIPAA Rules.

5. TERM AND TERMINATION.

- a. This Agreement shall be effective as of the date of the Contract to which this Agreement is attached, and shall terminate on the date BESSD terminates this Agreement or when all PHI is destroyed or returned to BESSD.
- b. In addition to any other remedies provided for by this Agreement or the Contract, upon the BESSD's knowledge of a material Breach by BUSINESS ASSOCIATE of this Agreement, the BUSINESS ASSOCIATE authorizes BESSD to do any one or more of the following, upon written notice to BUSINESS ASSOCIATE describing the violation and the action it intends to take:
 - (i) Exercise any of its rights to reports, access and inspection under this Agreement or the Contract;
 - (ii) Require BUSINESS ASSOCIATE to submit a plan of monitoring and reporting, as BESSD may determine necessary to maintain compliance with this Agreement;
 - (iii) Provide BUSINESS ASSOCIATE with a reasonable period of time to cure the Breach, given the nature and impact of the Breach; or
 - (iv) Immediately terminate this Agreement if BUSINESS ASSOCIATE has breached a material term of this Agreement and sufficient mitigation is not possible.²⁹
- c. Effect of Termination. Upon termination of this Agreement for any reason, until notified otherwise by BESSD, BUSINESS ASSOCIATE, with respect to PHI received from BESSD, or created, maintained, or received by BUSINESS ASSOCIATE on behalf of the BESSD, shall:
 - (i) Retain only that protected health information which is necessary for BUSINESS ASSOCIATE to continue its proper management and administration or to carry out its legal responsibilities;

²⁹ 45 CFR §164.504(e)(2)(iii)

- (ii) Return to BESSD or, if agreed to by BESSD and MQD, destroy, the remaining PHI that the BUSINESS ASSOCIATE still maintains in any form;
- (iii) Extend all protections, limitations, requirements and other provisions of this Agreement to all PHI and EPHI received from or on behalf of BESSD or created or received by BUSINESS ASSOCIATE on behalf of the BESSD, for as long as BUSINESS ASSOCIATE retains the PHI or EPHI, and ensure that these protections extend to PHI or EPHI created, received or maintained by Subcontractors of BUSINESS ASSOCIATE;
- (iv) Not use or disclose the PHI retained by BUSINESS ASSOCIATE other than for the purposes for which such PHI was retained and subject to the same conditions set out at section 3.c, above, which applied prior to termination; and
- (v) Return to the BESSD or, if agreed to by the STATE and MQD, destroy the PHI retained by BUSINESS ASSOCIATE when it is no longer needed by BUSINESS ASSOCIATE for its proper management and administration or to carry out its legal responsibilities.

6. MISCELLANEOUS.

- a. Amendment. BUSINESS ASSOCIATE and the BESSD 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 BESSD to comply with the HIPAA Rules. Notwithstanding the foregoing, nothing in this Agreement shall be interpreted to supercede 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 the Department of Human Services and the Department of Human Service's 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 or Subcontractors.
- d. Costs Related to Breach. BUSINESS ASSOCIATE shall be responsible for any and all costs incurred by BESSD or MQD 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 BUSINESS ASSOCIATE disclosed PHI under this Agreement, including but

not limited to notification of individuals or their representatives of a Breach of Unsecured PHI,³⁰ and the cost of mitigating any harmful effect of the Breach.³¹

- 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, MQD by BESSD, BUSINESS ASSOCIATE shall promptly forward a copy of such subpoena, notice or request to BESSD and MQD to afford MQD the opportunity to timely respond to the demand for its PHI as MQD determines appropriate according to its state and federal obligations.
- f. Survival. The respective rights and obligations of BESSD and BUSINESS ASSOCIATE under sections 5.c, Term and Termination, 6.c., Indemnification, and 6.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 and/or e-mailed to the appropriate address noted below. If notice is sent by e-mail, then a confirming written notice should be sent by mail and/or fax 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.

DHS Information Security / HIPAA
Compliance Manager
P.O. Box 700190
Kapolei, Hawaii 96709-0190
Fax: (808) 692-8173
Email: LYong@dhs.hawaii.gov

BUSINESS ASSOCIATE:

Fax: (_____) _____
Email: _____

³⁰ 45 CFR Part 164, Subpart D

³¹ 45 CFR §164.530(f)