



EXHIBIT _____

**BUSINESS ASSOCIATE and QUALIFIED SERVICE ORGANIZATION
("QSO") AGREEMENT**

State of Hawaii Department of Health,

(COVERED ENTITY)

and

(BUSINESS ASSOCIATE/QSO)

The State of Hawaii Department of Health, _____(COVERED ENTITY) has determined it is a Covered Entity or Health Care Component of 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).

_____ (BUSINESS ASSOCIATE/QSO) will provide COVERED ENTITY certain services described in the Contract to which this Exhibit ____ is attached and may have access to Protected Health Information (PHI) in fulfilling its responsibilities under the Contract.

To the extent BUSINESS ASSOCIATE/QSO needs to create, receive, maintain, or transmit PHI to perform services under the Contract, it will be acting as a Business Associate/QSO¹ of COVERED ENTITY and will be subject to the HIPAA Rules and terms of this Business Associate/QSO Agreement (Agreement).

¹ Definition of Business Associate, 45 CFR §160.103. Definition of Qualified Service Organization, 42 CFR §2.11.

COVERED ENTITY and BUSINESS ASSOCIATE/QSO (collectively referred to as “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 the manner not permitted by the Privacy Rule is presumed to be a Breach unless BUSINESS ASSOCIATE/QSO demonstrates to 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.

Breach excludes:

- A. Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under the authority of BUSINESS ASSOCIATE/QSO 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 BUSINESS ASSOCIATE/QSO to another person authorized to access PHI at the same BUSINESS ASSOCIATE/QSO, or organized health care arrangement in which COVERED ENTITY participates, 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 BUSINESS ASSOCIATE/QSO 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.

Business Associate³ means a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to,

² 45 CFR §164.402.

³ 45 CFR §160.102.

a Covered Entity. A member of COVERED ENTITY's Workforce is not a Business Associate.

Designated Record Set⁴ means records, including but not limited to PHI maintained, collected, used, or disseminated by or for 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 COVERED ENTITY to make decisions about Individuals.

Electronic Protected Health Information (EPHI)⁵ means PHI that is transmitted by Electronic Media⁶ or maintained in Electronic Media.

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

Individual⁷ means the person who is the subject of PHI and shall include a person who qualifies as a personal representative under 45 CFR §164.502(g) of the HIPAA Rules.

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.

Protected Health Information (PHI)⁸ 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, 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 is limited to the information created, maintained, received, or transmitted by BUSINESS ASSOCIATE/QSO on behalf of or from COVERED ENTITY. Protected Health Information includes without limitation EPHI, and excludes education records under 20 U.S.C. §1232(g), employment records held by COVERED ENTITY as an employer, and records regarding an Individual who has been deceased for more than 50 years.

Privacy Incident means any successful or unsuccessful attempt, loss of control, compromise, or unauthorized use, disclosure, acquisition, or access of PHI.

Security Incident⁹ means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System.

⁴ 45 CFR §164.501.

⁵ 45 CFR §160.103.

⁶ Ibid.

⁷ Ibid.

⁸ Ibid.

⁹ 45 CFR §164.304.

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

Unsecured Protected Health Information (Unsecured PHI)¹⁰ 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.

Workforce¹¹ means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for COVERED ENTITY or BUSINESS ASSOCIATE/QSO and is under the direct control of such, whether or not they are paid by COVERED ENTITY or BUSINESS ASSOCIATE.

2. BUSINESS ASSOCIATE/QSO'S OBLIGATIONS.

BUSINESS ASSOCIATE/QSO agrees to:

- a. 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/QSO use or further disclose PHI in a manner that would violate the Privacy Rule if done by COVERED ENTITY, except as expressly provided in this Agreement.¹²
- b. Implement appropriate safeguards, and comply, where applicable, with the Security Rule to ensure the confidentiality, integrity, and availability of all EPHI BUSINESS ASSOCIATE/QSO creates, receives, maintains, or transmits on behalf of COVERED ENTITY; protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI; prevent use or disclosure of EPHI other than as provided for by this Agreement or as Required By Law; and ensure compliance with the HIPAA Rules by BUSINESS ASSOCIATE/QSO's Workforce.¹³ These safeguards include, but are not limited to:
 - (i) Administrative Safeguards. BUSINESS ASSOCIATE/QSO 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 enforcing those policies and procedures, including sanctions for anyone not found in compliance.
 - (ii) Technical and Physical Safeguards. BUSINESS ASSOCIATE/QSO shall implement appropriate technical safeguards to protect EPHI, including access controls, authentication, and transmission security,

¹⁰ 45 CFR §164.402.

¹¹ 45 CFR §160.103.

¹² 45 CFR §§164.502(a)(3); 164.504(e)(2)(ii)(A).

¹³ 45 CFR §164.306(a).

as well as implement appropriate physical safeguards to protect EPHI, including workstation security and device and media controls;¹⁴ and

- (iii) Training. BUSINESS ASSOCIATE/QSO shall provide training to relevant Workforce members, including management, on how to prevent the improper access, use, or disclosure of EPHI; and update and repeat training on a regular basis.¹⁵
- c. 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/QSO's safeguards. BUSINESS ASSOCIATE/QSO 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.¹⁶
 - d. Comply with the provisions found in 45 CFR §164.308(a)(1)(ii)(A) and (B), requiring BUSINESS ASSOCIATE/QSO to conduct an accurate and thorough Risk Analysis, and to periodically update the Risk Analysis (no less than once every 3 years); and to implement Risk Management measures to reduce the risk and vulnerabilities to a reasonable and appropriate level to comply with 45 CFR §164.306(a).
 - e. Ensure that any subcontractor of BUSINESS ASSOCIATE/QSO that creates, receives, maintains, or transmits PHI on behalf of BUSINESS ASSOCIATE/QSO agrees in writing to the same restrictions, conditions and requirements that apply to BUSINESS ASSOCIATE/QSO through this Agreement with respect to such PHI.¹⁷
 - f. Notify COVERED ENTITY following discovery of any use or disclosure of PHI not permitted by this Agreement including any incidents of which it becomes aware, or any Breach of Unsecured PHI.¹⁸
 - (i) BUSINESS ASSOCIATE/QSO shall immediately notify COVERED ENTITY's HIPAA Privacy and/or Security Officer verbally.
 - (ii) BUSINESS ASSOCIATE/QSO shall subsequently notify COVERED ENTITY's HIPAA Privacy and/or Security Officer 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, Security Incident, or Breach of Unsecured PHI.
 - (iii) BUSINESS ASSOCIATE/QSO shall make additional information available upon request from COVERED ENTITY.
 - (iv) A Breach of Unsecured PHI shall be treated as discovered by BUSINESS ASSOCIATE/QSO as of the first day on which such Breach is known to BUSINESS ASSOCIATE/QSO. BUSINESS ASSOCIATE/QSO 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

¹⁴ 45 CFR §§164.310; 164.312.

¹⁵ 45 CFR §164.308(a)(5).

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

¹⁷ 45 CFR §§164.308(b); 164.314(a)(2); 164.502(e); 164.504(e)(2)(ii)(D).

¹⁸ 45 CFR §§164.314(a)(2); 164.410(a); 164.504(e)(2)(ii)(C).

the Breach, who is an employee, officer, Workforce member, or other agent of BUSINESS ASSOCIATE/QSO.¹⁹

- g. Take prompt corrective action to mitigate, to the extent practicable, any harmful effect that is known to BUSINESS ASSOCIATE/QSO of a Security Incident or a misuse or unauthorized disclosure of PHI by BUSINESS ASSOCIATE/QSO 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/QSO shall reasonably cooperate with 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.²⁰
- h. Investigate such Breach and provide a written report of the investigation and resultant mitigation to COVERED ENTITY's HIPAA Privacy and/or Security Officer as soon as practicable, but no longer than thirty (30) calendar days of the discovery of the Breach.
- i. Provide the following information with respect to a Breach of Unsecured PHI, to the extent possible, as the information becomes available, to COVERED ENTITY'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/QSO to have been accessed, acquired, used, or disclosed during the Breach; and
 - (ii) Any other available information that COVERED ENTITY is required to include in notification to the Individual under the HIPAA Rules, including, but not limited to the following:²¹
 - A. If known to BUSINESS ASSOCIATE/QSO, contact information for Individuals who were or who may have been impacted by the Breach (including but not limited to: 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. 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 BUSINESS ASSOCIATE/QSO 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

¹⁹ 45 CFR §164.410(a)(2).

²⁰ 45 CFR §§164.308(a)(6); 164.530(f).

²¹ 45 CFR §§164.404(c)(1); 164.408; 164.410(c)(1) and (2).

- E. Contact information for BUSINESS ASSOCIATE/QSO's liaison responsible for investigating the Breach and communicating information relating to the Breach to COVERED ENTITY.
- j. Promptly report to COVERED ENTITY's HIPAA Privacy and/or Security Officer any Security Incident of which BUSINESS ASSOCIATE/QSO becomes aware with respect to EPHI that is in the custody of BUSINESS ASSOCIATE/QSO, including Breaches of Unsecured PHI as required by 45 CFR §164.410, by contacting the HIPAA Privacy and/or Security Officer.²²
- k. 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 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.²³
- l. Make its internal policies, procedures, books, and records relating to the use and disclosure of PHI received from, created, or received by BUSINESS ASSOCIATE/QSO on behalf of COVERED ENTITY available to the U.S. Secretary of Health and Human Services or to COVERED ENTITY if necessary or required to assess BUSINESS ASSOCIATE/QSO's or COVERED ENTITY's compliance with the HIPAA Rules. BUSINESS ASSOCIATE/QSO shall promptly notify COVERED ENTITY of communications with the U.S. Department of Health and Human Services (HHS) regarding PHI provided by or created on behalf of COVERED ENTITY and shall provide COVERED ENTITY with copies of any information BUSINESS ASSOCIATE/QSO has made available to HHS under this paragraph.²⁴
- m. 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.²⁵
- n. Make available PHI held by BUSINESS ASSOCIATE/QSO, which COVERED ENTITY has determined to be part of its Designated Record Set, to COVERED ENTITY as necessary to satisfy COVERED ENTITY's obligations to provide an Individual with access to PHI under 45 CFR §164.524, in the time and manner designated by COVERED ENTITY.²⁶
- o. Make available PHI held by BUSINESS ASSOCIATE/QSO, which COVERED ENTITY has determined to be part of its Designated Record Set, for amendment and incorporate any amendments to PHI that COVERED ENTITY directs or agrees to in accordance with 45 CFR §164.526, upon request of COVERED ENTITY or the Individual.

²² 45 CFR §§164.314(a)(2); 164.410.

²³ 45 CFR §§164.308(a).

²⁴ 45 CFR §164.504(e)(2)(ii)(I).

²⁵ 45 CFR §164.522.

²⁶ 45 CFR §§164.504(e)(2)(ii)(E); 164.524.

- p. Document disclosures of PHI made by BUSINESS ASSOCIATE/QSO, which are required to be accounted for under 45 CFR §164.528(a)(1), and make this information available as necessary to satisfy COVERED ENTITY's obligation to provide an accounting of disclosures to an Individual within two (2) business days' notice by COVERED ENTITY of a request by an Individual for an accounting of disclosures of PHI. If an Individual directly requests an accounting of disclosures of PHI from BUSINESS ASSOCIATE/QSO, BUSINESS ASSOCIATE/QSO shall notify COVERED ENTITY's HIPAA Privacy and/or Security Officer of the request within two (2) business days, and COVERED ENTITY shall either direct BUSINESS ASSOCIATE/QSO 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.²⁷
- q. Comply with any other requirements of the HIPAA Rules not expressly specified in this Agreement, as to the extent that such requirements apply to BUSINESS ASSOCIATE/QSOs under the HIPAA Rules, as the same may be amended from time to time.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE/QSO.

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 COVERED ENTITY or violate the Minimum Necessary requirements applicable to COVERED ENTITY.²⁸
- b. Limited Use of PHI for BUSINESS ASSOCIATE/QSO's Benefit. Use the PHI received by BUSINESS ASSOCIATE/QSO in its capacity as COVERED ENTITY's BUSINESS ASSOCIATE/QSO, if necessary, for the proper management and administration of BUSINESS ASSOCIATE/QSO or to carry out the legal responsibilities of BUSINESS ASSOCIATE/QSO. BUSINESS ASSOCIATE/QSO's proper management and administration does not include the use or disclosure of PHI by BUSINESS ASSOCIATE/QSO for Marketing purposes or for Sale of PHI.²⁹
- c. Limited Disclosure of PHI for BUSINESS ASSOCIATE/QSO's Benefit. Disclose PHI for BUSINESS ASSOCIATE/QSO's proper management and administration or to carry out its legal responsibilities only if the disclosure is Required By Law,³⁰ or BUSINESS ASSOCIATE/QSO obtains reasonable assurances from the 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 entity,

²⁷ 45 CFR §§164.504(e)(2)(ii)(G) and (H), 164.528; HAR §2-71-11 through -20.

²⁸ 45 CFR §§164.502(a) and (b); 164.504(e)(2)(i).

²⁹ 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).

³⁰ E.g., 45 CFR Parts 170 and 171; 42 CFR Part 2, etc.

and the entity notifies BUSINESS ASSOCIATE/QSO of any instances of which it is aware in which the confidentiality of PHI has been Breached.³¹

- d. Minimum Necessary. BUSINESS ASSOCIATE/QSO shall only request, use, and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure.³²
- e. Data Aggregation. Use PHI to provide Data Aggregation services relating to COVERED ENTITY's Health Care Operations as permitted by 45 CFR §164.504(e)(2)(i)(B).
- f. Disclosures by Whistleblowers. Disclose PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

4. COVERED ENTITY'S OBLIGATIONS.

- a. COVERED ENTITY shall not request BUSINESS ASSOCIATE/QSO to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by COVERED ENTITY.
- b. COVERED ENTITY shall not provide BUSINESS ASSOCIATE/QSO with more PHI than is minimally necessary for BUSINESS ASSOCIATE/QSO to provide the services under the Contract and this Agreement and COVERED ENTITY shall provide any PHI needed by BUSINESS ASSOCIATE/QSO to perform its obligations in accordance with the HIPAA Rules.

5. QUALIFIED SERVICE ORGANIZATION ("QSO")³³ PROVISIONS.

- a. BUSINESS ASSOCIATE/QSO is fully bound by 42 CFR Part 2 in receiving, storing, processing, or otherwise dealing with any information from the Part 2 program about Individuals; and
- b. BUSINESS ASSOCIATE/QSO shall resist in judicial proceedings, if necessary, any efforts to obtain access to Individual-identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by 42 CFR Part 2.

³¹ 45 CFR §164.504(e)(4)(ii).

³² 45 CFR §164.502(b).

³³ Qualified Service Organization is defined at 42 CFR §2.11.

6. TERM AND TERMINATION.

- a. This Agreement shall be effective as of the date it is signed by BUSINESS ASSOCIATE/QSO, and shall terminate on the date COVERED ENTITY terminates this Agreement or when all PHI is destroyed or returned to COVERED ENTITY.
- b. In addition to any other remedies provided for by this Agreement, upon COVERED ENTITY's knowledge of a material breach by BUSINESS ASSOCIATE/QSO of this Agreement, BUSINESS ASSOCIATE/QSO authorizes COVERED ENTITY to do any one or more of the following, upon written notice to BUSINESS ASSOCIATE/QSO describing the violation and the action it intends to take:
- (i) Exercise any of its rights to reports, access, and inspection under this Agreement;
 - (ii) Require BUSINESS ASSOCIATE/QSO to submit a plan of monitoring and reporting, as COVERED ENTITY may determine necessary to maintain compliance with this Agreement;
 - (iii) Provide BUSINESS ASSOCIATE/QSO 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/QSO has breached a material term of this Agreement and sufficient mitigation is not possible.³⁴
- c. Effect of Termination.³⁵
- (i) Upon termination of this Agreement, until notified otherwise by COVERED ENTITY, BUSINESS ASSOCIATE/QSO shall extend all protections, limitations, requirements, and other provisions of this Agreement to all EPHI received from or on behalf of COVERED ENTITY or created or received by BUSINESS ASSOCIATE/QSO on behalf of COVERED ENTITY, and all EPHI created, received, maintained, or transmitted by BUSINESS ASSOCIATE/QSO on behalf of COVERED ENTITY.
 - (ii) Except as otherwise provided in §6(c)(iii) below, upon termination of this Agreement for any reason, BUSINESS ASSOCIATE/QSO shall, at COVERED ENTITY's option, return or destroy all PHI received from COVERED ENTITY, or created or received by BUSINESS ASSOCIATE/QSO on behalf of COVERED ENTITY, that BUSINESS ASSOCIATE/QSO still maintains in any form, and BUSINESS ASSOCIATE/QSO shall retain no copies of the PHI. This provision shall also apply to PHI that is in the possession of subcontractors or agents of BUSINESS ASSOCIATE/QSO. BUSINESS ASSOCIATE/QSO shall notify COVERED ENTITY in writing of any and all conditions that make return or destruction of such information

³⁴ 45 CFR §164.504(e)(2)(iii).

³⁵ 45 CFR §164.504(e)(2)(ii)(J).

not feasible and shall provide COVERED ENTITY with any requested information related to COVERED ENTITY's determination as to whether the return or destruction of such information is feasible.

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

7. MISCELLANEOUS.

- a. Amendment. BUSINESS ASSOCIATE/QSO and COVERED ENTITY 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 COVERED ENTITY 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/QSO shall defend, indemnify, and hold harmless COVERED ENTITY and COVERED ENTITY's officers, employees, agents, contractors, and subcontractors to the extent required under this Agreement and 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/QSO or any of BUSINESS ASSOCIATE/QSO's officers, employees, agents, contractors, or subcontractors. This indemnification provision shall not apply to any BUSINESS ASSOCIATE/QSO that is another Hawaii government entity; however, BUSINESS ASSOCIATE/QSO shall seek indemnification for COVERED ENTITY from BUSINESS ASSOCIATE/QSO's agents, contractors, or subcontractors that are not Hawaii government entities.

- d. Costs Related to Breach. BUSINESS ASSOCIATE/QSO shall be responsible for any and all costs incurred by COVERED ENTITY as a result of any Breach of PHI by BUSINESS ASSOCIATE/QSO, its officers, directors, employees, contractors or agents, or by a third party to which BUSINESS ASSOCIATE/QSO disclosed PHI under this Agreement, including but not limited to notification of individuals or their representatives of a Breach of Unsecured PHI,³⁶ and the cost of mitigating any harmful effect of the Breach.³⁷ Providing notice to the individuals of a Breach will be the responsibility of COVERED ENTITY.
- e. Response to Subpoenas. In the event BUSINESS ASSOCIATE/QSO receives a subpoena or similar notice or request from any judicial, administrative or other party which would require the production of PHI received from, created or maintained for COVERED ENTITY, BUSINESS ASSOCIATE/QSO shall promptly forward a copy of such subpoena, notice, or request to COVERED ENTITY to afford COVERED ENTITY the opportunity to timely respond to the demand for its PHI as COVERED ENTITY determines appropriate according to its State and Federal obligations.
- f. Survival. The respective rights and obligations of COVERED ENTITY and BUSINESS ASSOCIATE/QSO under §6.c, Term and Termination, §7.c, Indemnification, and §7.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. Notice shall be sent to the telephone and fax numbers, mailing, email addresses listed below:
- h. Breach Notification to COVERED ENTITY's Officers. Pursuant to §§2(f)(i), (ii) and (iii) of this Agreement, should BUSINESS ASSOCIATE/QSO or its subcontractor(s) breach COVERED ENTITY's PHI, BUSINESS ASSOCIATE/QSO shall contact:

³⁶ 45 CFR Part 164, Subpart D.

³⁷ 45 CFR §164.530(f).

COVERED ENTITY HIPAA OFFICER:

HIPAA Privacy Officer
1250 Punchbowl Street, Room 250
Honolulu, Hawaii 96813
Phone: (808) 586-4111
Fax: (808) 586-4115
Email: gino.merez@doh.hawaii.gov

BUSINESS ASSOCIATE/QSO HIPAA CONTACT:

BUSINESS ASSOCIATE/QSO

Date: _____

Signature: _____

Print Name: _____

Title: _____

COVERED ENTITY

Date: _____

Signature: _____

Print Name: _____

Title: _____