MEMORANDUM OF UNDERSTANDING

BETWEEN

INLAND EMPIRE HEALTH PLAN

AND

SILVER VALLEY UNIFIED SCHOOL DISTRICT

MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding ("MOU") is made and entered into by and between Inland Empire Health Plan ("IEHP"), a local public entity of the State of California, and Silver Valley Unified School District (SVUSD) ("CONTRACTOR"), with references to the following facts:

WHEREAS, CONTRACTOR and IEHP will collaborate for the purpose of the Healthy School Program to provide targeted services to SVUSD students that are IEHP Members and non-members; and

WHEREAS, the Healthy School Program will promote appropriate utilization of benefits, provide healthcare access navigation, and will connect families with community resources and internal IEHP departments based on their identified needs.

NOW THEREFORE, in consideration of the mutual covenants contained herein, the Parties agree as follows:

1. SERVICES

A. Description Of Services. CONTRACTOR shall provide IEHP with identified SVUSD students information such as: name, date of birth, health insurance information (if applicable), parent's contact information for the purpose of the Healthy School Program to provide necessary services as set forth in Attachment A, attached hereto, and incorporated herein by reference.

B. Scope Of Services. CONTRACTOR shall furnish labor necessary to perform in a complete, skillful and professional manner all those services described in Attachment A.

2. PERIOD OF PERFORMANCE

The term of this Agreement shall become effective as of date of last signature and shall continue in effect for an initial term of June 30, 2026 unless terminated as specified in Section 7 (TERMINATION PROVISION).

3. COMPENSATION

No compensation will be exchanged between the parties. CONTRACTOR shall offer the services as indicated in Attachment A.

4. INDEPENDENT CONTRACTOR

It is understood and agreed that CONTRACTOR is an independent contractor and that no relationship of employer-employee exists between the parties hereto. Neither party's officers, agents, employees or subcontractors, shall be entitled to any benefits payable to employees of the other party, including Workers' Compensation Benefits.

5. INDEMNIFICATION

CONTRACTOR shall indemnify, and hold harmless IEHP, its officers, employees and agents from any liability whatsoever, including wrongful death, based or asserted upon any act or omission of the CONTRACTOR, its employees, subcontractors and agents relating to or in any way connected with the accomplishment of the work or performance of service under this Agreement. As part of the foregoing indemnity, CONTRACTOR agrees to protect and defend at its own expense, including attorneys' fees, IEHP, its officers, agents and employees in any legal action based upon any such alleged acts or omissions. The terms of this Section shall survive the termination of this Agreement.

6. INSURANCE

Throughout the term of this Agreement, CONTRACTOR shall maintain, at its sole cost and expense, insurance coverage CONTRACTOR deems prudent and customary in the exercise of CONTRACTOR's business operations, in amounts as may be necessary to protect CONTRACTOR and its officers, agents, and employees, as applicable, in the discharge of its responsibilities and obligations under this Agreement.

7. TERMINATION PROVISION

A. Either party may terminate this Agreement, without cause, upon fifteen (15) days written notice served upon the other party.

B. Should IEHP determine that there is a basis for termination for cause; such termination shall be effected upon five (5) days written notice to CONTRACTOR.

8. NONDISCRIMINATION

CONTRACTOR shall not discriminate on the basis of race, color, national origin, ancestry, religion, sex, marital status, sexual orientation, income, health status or age in the performance of this Agreement, and, to the extent they shall be found to be applicable hereto, shall comply with the provisions of the Fair Employment and Housing Act (commencing with Section 12900 *et seq.* of the Government Code), and Federal Civil Rights Act of 1964 (P.L. 88-352).

9. CONFLICT OF INTEREST

CONTRACTOR shall have no interest, and shall not acquire any interest, direct or indirect, which will unlawfully conflict in any manner or degree with the performance of services required under this Agreement.

10. PROTECTED HEALTH INFORMATION ("PHI")

In the event that there is PHI shared between IEHP and CONTRACTOR pursuant this Agreement, IEHP and CONTRACTOR are subject to all relevant requirements contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), codified at Title 45, C.F.R., Parts 160 and 164, the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009 (HITECH), Public Law 111-5, enacted February 17, 2009, and the laws and regulations promulgated subsequent hereto and as amended, for purposes of services rendered pursuant to the Agreement. The Parties agree to cooperate in accordance with the terms and intent of this Agreement for implementation of relevant law(s) and/or regulation(s) promulgated under HIPAA and HITECH. The Parties further agree that it shall be in compliance with the requirements of HIPAA, HITECH, and the laws and regulations promulgated subsequent hereto and as amended. CONTRACTOR further agrees to the provisions of the HIPAA Business Associate Agreement, attached hereto in Attachment B, and incorporated herein by this reference.

11. NOTICES

All correspondence and notices required or contemplated by this Agreement shall be delivered to the respective parties at the addresses set forth below, or to such other address(es) the parties may hereafter designate in writing. Delivery and are deemed submitted one day after their deposit in the United States mail, postage prepaid:

IEHP:

Jarrod McNaughton, MBA, FACHE
Chief Executive Officer
10801 Sixth Street
Rancho Cucamonga, CA 91730
(909) 890-2000
cc: IEHP Legal Department

CONTRACTOR:

Jesse Najera
Superintendent
35320 Daggett-Yermo Rd
Yermo, CA 92398
760-254-2916

or to such other address(es) as the parties may hereafter designate, in writing.

12. SEVERABILITY

The provisions of this Agreement are severable, in whole or in part, and if any part is found to be unenforceable, the other parts shall remain fully valid and enforceable.

13. WAIVER

Waiver by either party of any breach of any one (1) or more of the terms of this Agreement shall not be construed to be a waiver of any subsequent or other breach of the same term or of any other term herein.

14. GOVERNING LAW; VENUE

A. This Agreement is made and entered into in the State of California and shall be construed under the laws of the State of California excluding its conflicts of law provisions. The provisions of the Government Claims Act (Government Code Section 900, *et seq.*) must be followed first for any disputes under this Agreement.

B. All actions and proceedings arising in connection with this Agreement shall be tried and litigated exclusively in the state or federal (if permitted by law and a party elects to file an action in federal court) courts located in the counties of San Bernardino or Riverside, State of California.

15. LIMITATION OF LIABILITY

Without affecting the indemnification obligations set forth in this Agreement, in no event shall either party be liable for consequential, indirect, or incidental damages, including, without limitation, lost profits, arising out of the services provided under this Agreement.

16. COUNTERPARTS; SIGNATURE

This Agreement may be executed in one or more duplicates or counterparts, any one of which shall be deemed to be the original. The Parties' faxed signatures, and/or signatures scanned into PDF format, shall be effective to bind them to this Agreement.

17. ENTIRE AGREEMENT

This Agreement, including all attachments and manuals, is the entire agreement between the Parties, supersedes all prior agreements, promises, negotiations or representations, either oral or written between the Parties with respect to the subject matter and period governed by this Agreement. This Agreement may not be assigned or delegated, either in whole or in part,

amended, changed, terminated or modified in any respect or particular, unless the same shall be in writing and signed by the party charged.

18. COMPLIANCE WITH LAW

The parties shall observe and comply with all applicable local, state and federal laws, ordinances, rules and regulations now in effect or hereafter enacted, each of which is hereby made a part hereof and incorporated herein by reference.

19. CERTIFICATION OF AUTHORITY TO EXECUTE THIS AGREEMENT

CONTRACTOR certifies that the individual signing below has authority to execute this Agreement on behalf of CONTRACTOR, and may legally bind CONTRACTOR to the terms and conditions of this Agreement, and any attachments hereto.

[SIGNATURES ON FOLLOWING PAGE]

IN WITNESS WHEREOF, the parties hereto have executed this Memorandum of Understanding in as set forth below.

SILVER VALLEY UNIFIED SCHOOL DISTRICT

By: _____
Jesse Najera
Superintendent

Date: _____

INLAND EMPIRE HEALTH PLAN:

By: _____
Jarrod McNaughton, MBA, FACHE
Chief Executive Officer

Date: _____

By: _____
Vice Chair, IEHP Governing Board

Date: _____

Attest: _____
Secretary, IEHP Governing Board

Date: _____

Approved as to Form:

By: _____
Anna W. Wang
Vice President, General Counsel

Date: _____

ATTACHMENT A

SCOPE OF SERVICES

1. CONTRACTOR shall perform the services as described below:

    A. Staff from CONTRACTOR's selected schools will refer students, both IEHP Members and non-members, seeking health insurance assistance to a IEHP Health Navigator (HN) via a secure email.

    B. Staff from CONTRACTOR's selected school will assist with marketing of the Health Navigator program by including program information on school's social media accounts, posting flyers on school campus, and adding electronic/on-screen flyers in lobby area.

    C. When HN is onsite at a school, school staff will designate appropriate office space (table, chair, phone line, if applicable) with Covid-19 safety and PHI privacy guidelines, in order to conduct 1:1 meetings with families.

    D. Staff from CONTRACTOR's selected school will provide HN a list of students that meet the following criteria: active IEHP member, missing immunizations, chronic absenteeism, behavioral health concerns, or Social Determinants of Health (SDOH) needs.

2. IEHP Responsibilities:

    A. IEHP's HN team will visit selected schools onsite on a weekly basis to coach school staff on the Healthy School Program (HSP) and discuss upcoming events and presentations.

    B. IEHP's HN will collaborate with onsite school staff and refer to school, Managed Care Plan (MCP), or community programs that support the care coordination of services rendered and address students' health, behavioral or social needs.

    C. HN(s) will be onsite at a selected school on a weekly basis to assist families who have been referred to IEHP for health, behavioral or social needs. The HN shall perform the following services for each referral:

        a. HN will schedule a face-to-face appointment with members at their preferred location (i.e., home visit, school site, community setting) and will conduct a screener to determine their needs: mental, physical, and social determinants of health.

b. HN will pre-screen IEHP non-members and redirect based on their needs to Community Based Organizations (CBOs) and IEHP Medi-Cal Eligibility Continuity department.

c. IEHP will provide a quarterly report of IEHP members and non-members referred and participation status.

d. HN will categorize IEHP Members into one of the three (3) tiers based on Member needs:

- Tier 1
    a. Members with basic assistance needs. For example:
        i. Provide benefit information such as: Nurse Advice Line, Urgent Care Clinics, and Access to Care
        ii. Ordering IEHP Member Card
        iii. Assistance with IEHP transportation
        iv. Assistance with PCP change
- Tier 2
    a. Members with intermediate assistance needs. For example:
        i. Provide benefit information such as: Nurse Advice Line, Urgent Care Clinics, and Access to Care
        ii. Scheduling PCP and Specialist (vision, dental, behavioral health, and specialty care) appointments
        iii. Enrollment in Health Education classes
        iv. Follow-up needed after first interaction
- Tier 3
    a. Members with high assistance needs. For example:
        i. Provide benefit information such as: Nurse Advice Line, Urgent Care Clinics, and Access to Care
        ii. Assistance with Specialist follow-up appointments as needed

iii. Accompaniment to appointments if needed

iv. Two or more follow-ups needed after first interaction

D. HN will send out a monthly email to all assigned/virtual schools to share IEHP Community Resource Centers (CRC) calendar of classes, new local resources, upcoming events, and share secure email and virtual referral process.

E. HN will collaborate with school staff and provide an IEHP Benefit Overview and any requested trainings (Ex. How to Use ConnectIE, CRC Information, Applied Suicide Intervention Skills Training [ASIST])

F. HN will provide IEHP Benefit Overview to families, help identify social determinants of health barriers, and connect them to applicable CBOs.

G. HN will connect families to identified behavioral health resources based on screener.

2. Except as otherwise indicated in this Agreement, CONTRACTOR shall provide (at Contractor's expense) all equipment, tools, and other materials necessary to provide the services indicated herein.

ATTACHMENT B

HIPAA BUSINESS ASSOCIATE AGREEMENT

INLAND EMPIRE HEALTH PLAN

SILVER VALLEY UNIFIED SCHOOL DISTRICT

This HIPAA Business Associate Agreement (the "Agreement") is made and entered into as of date of last signature ("Effective Date") by and between the Inland Empire Health Plan ("IEHP") and Silver Valley Unified School District ("Business Associate") with reference to the following facts:

RECITALS

WHEREAS, IEHP and Business Associate entered into this Agreement pursuant to which Business Associate provides services to IEHP, and in conjunction with the provision of such services, certain Protected Health Information ("PHI") and/or certain electronic Protected Health Information ("ePHI") may be made available to Business Associate for the purposes of carrying out its obligations under the Agreement; and,

WHEREAS, the provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), more specifically the regulations found in Title 45, C.F.R., Parts 160 and 164, Subparts A and E (the "Privacy Rule") and/or 45 C.F.R. Part 164, Subpart C (the "Security Rule"), as may be amended from time to time, which are applicable to the protection of any disclosure or use of PHI and/or ePHI pursuant to this Agreement; and,

WHEREAS, the provisions of Subtitle D entitled "Privacy" of the Health Information Technology for Economic and Clinical Health Act ("HITECH") of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, and the implementing regulations adopted thereunder, as may be amended from time to time, impose certain requirements on business associates; and

WHEREAS, the provisions of the California Information Practices Act, more specifically found in California Civil Code sections 1798-1798.98; the Confidentiality of Alcohol and Drug Abuse Patient Records, found in Title 42 C.F.R. Part 2, the California Welfare and Institutions Code section 5328, and the California Health and Safety Code section 11845.5, as may be amended from time to time, which are applicable to the use of certain PHI and/or confidential information; and

WHEREAS, IEHP is a Covered Entity, as defined in the Privacy Rule; and,

WHEREAS, Business Associate, when on behalf of IEHP, creates, receives, maintains or transmits PHI and/or ePHI, is a business associate as defined in the Privacy Rule; and,

WHEREAS, the parties intend to enter into this Agreement to address the requirements of HIPAA, HITECH, Privacy Rule, and Security Rule as they apply to Business Associate as a business associate of IEHP, including the establishment of permitted and required uses and disclosures (and appropriate limitations and conditions on such uses and disclosures) of PHI and/or ePHI by Business Associate that is created or received in the course of performing services on behalf of IEHP, and to incorporate the business associate obligations set forth in HITECH; and,

WHEREAS, the parties agree that any disclosure or use of PHI and/or ePHI be in compliance with the Privacy Rule, Security Rule, HITECH, or other applicable law;

WHEREAS, IEHP, on behalf of the California Department of Health Care Services ("DHCS"), provides services or arranges, performs, or assists in the performance of functions or activities on behalf of DHCS, and may create, receive, maintain, transmit, aggregate, use or disclose PHI in order to fulfill IEHP's obligations under DHCS' contract;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

A. **DEFINITIONS**

B. Unless otherwise provided in this Agreement, or specifically defined in Paragraph B of this Section 1, the capitalized terms shall have the same meanings as set forth in the Privacy Rule, Security Rule, and/or HITECH, as may be amended from time to time.

1. Specific Definitions:

a. "Breach," when used in connection with Unsecured PHI, means, as defined in 45 C.F.R. § 164.402, the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule (45 C.F.R. Part 164, Subpart E), which compromises the security or privacy of the PHI. Except as otherwise excluded under 45 C.F.R. § 164.402, such acquisition, access, use or disclosure is presumed to be a Breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

b. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

c. The unauthorized person who used the PHI or to whom the disclosure was made;

d. Whether the PHI was actually acquired or viewed; and

2. The extent to which the risk to PHI has been mitigated.

3. "Discovered" means the first day on which such Breach is known to such Covered Entity or Business Associate, respectively, (including any person, other than the individual committing the Breach, that is an employee, officer or other agent of such entity or associate, respectively) or should reasonably have been known to such Covered Entity or Business Associate (or person) to have occurred.

4. "Electronic Protected Health Information" ("ePHI") means, as defined in 45 C.F.R. § 160.103, PHI transmitted by or maintained in electronic media, and for purposes of this Agreement, is limited to the ePHI that Business Associate creates, receives, maintains or transmits on behalf of IEHP.

5. "Protected Health Information" ("PHI") shall generally have the meaning given such term in 45 C.F.R. § 160.103, which includes ePHI, and for purposes of this Agreement, is limited to PHI, including ePHI, that Business Associate creates, receives, maintains or transmits on behalf of IEHP.

6. "Secretary" means the Secretary of the U.S. Department of Health and Human Services or his/her designee.

7. "Subcontractor" means a person to whom a business associate delegates a function, activity, or service other than in the capacity of a member of the workforce of such business associate.

2. "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under 42 U.S.C. § 17932(h)(2).

A. **SCOPE OF USE AND DISCLOSURE BY BUSINESS ASSOCIATE OF PHI AND/OR EPHI**

1. Business Associate shall be permitted to use PHI and/or ePHI disclosed to it by IEHP:

2. On behalf of IEHP, or to provide services to IEHP for the purposes contained herein, if such use or disclosure would not violate the Privacy Rule, Security Rule, and/or HITECH.

B. As necessary to perform any and all of its obligations under this Agreement for the following stated purposes:
for the purpose of the Healthy School Program to provide necessary services as set forth in Attachment A, attached hereto.

1. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or required by this Agreement or required by law, Business Associate may:

2. Use the PHI and/or ePHI in its possession for its proper management and administration and to fulfill any legal obligations.

a. Disclose the PHI and/or ePHI in its possession to a third party for the purpose of Business Associate's proper management and administration or to fulfill any legal responsibilities of Business Associate, only if:

b. The disclosure is required by law; or

i. Business Associate obtains written assurances from any person or organization to which Business Associate will disclose such PHI and/or ePHI that the person or organization will:

ii. Hold such PHI and/or ePHI in confidence and use or further disclose it only for the purpose of which Business Associate disclosed it to the third party, or as required by law; and

3. Notify Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been breached.

4. Use the PHI and/or ePHI to provide Data Aggregation services relating to the Health Care Operations of IEHP if authorized by this Agreement or pursuant to the written request of IEHP.

C. De-identify any and all PHI and/or ePHI of IEHP received by Business Associate under this Agreement provided that the De-identification conforms to the requirements of the Privacy Rule and/or Security Rule and does not preclude timely payment and/or claims processing and receipt.

1. Business Associate shall not:

2. Use or disclose PHI and/or ePHI it receives from IEHP, nor from another business associate of IEHP, except as permitted or required by this Agreement, or as required by law.

3. Perform any services (including any and all subcontracted services), which involves creating, receiving, maintaining or transmitting PHI and/or ePHI outside the United States of America.

4. Disclose PHI and/or ePHI not authorized by this Agreement without patient authorization or De-identification of the PHI and/or ePHI as authorized in writing by IEHP.

5. Make any disclosure of PHI and/or ePHI that IEHP would be prohibited from making.

6. Use or disclose PHI for fundraising or marketing purposes.

7. Disclose PHI, except as otherwise required by law, to a health plan for payment or healthcare operations purposes if the individual has requested this restriction, and the PHI solely relates to a health care item or service that is paid in full by the individual or person (other than the health plan) on behalf of the individual (45 C.F.R. § 164.522(a)(1)(vi)).

8. Directly or indirectly receive remuneration in exchange for PHI nor engage in any acts that would constitute a Sale of PHI, as defined in 45 C.F.R. § 164.502(a)(5)(ii), except with the prior written consent of IEHP and as permitted by and in compliance with 45 C.F.R. § 164.508(a)(4); however, this prohibition shall not affect payment by IEHP to Business Associate for services provided pursuant to this Agreement.

9. Use or disclose PHI that is Genetic Information for Underwriting Purposes, as those terms are defined in 45 C.F.R. §§ 160.103 and 164.502(a)(5)(i), respectively.

D. Divulge the Medi-Cal status of IEHP's Members without DHCS' prior approval except for treatment, payment, and operations, or as required by law.

E. Business Associate agrees that in any instance where applicable state and/or federal laws and/or regulations are more stringent in their

requirements than the provisions of HIPAA and/or HITECH (including but not limited to prohibiting the disclosure of mental health, and/or substance abuse records), the more stringent laws and/or regulations shall control the disclosure of PHI. Any provision of this Agreement which is in conflict with current or future applicable Federal or State laws is hereby amended to conform to the provisions of those laws. Such amendment of this Agreement shall be effective on the effective date of the laws necessitating it, and shall be binding on the parties even though such amendment may not have been reduced to writing and formally agreed upon and executed by the parties.

3. Business Associate must provide DHCS with a list of external entities, including persons, organizations, and agencies, other than those within its treatment network and other then DHCS, to which it discloses lists of Medi-Cal Member names and addresses. Business Associate must provide DHCS with the list within 30 calendar days of the execution of this Agreement and annually thereafter.

A. **OBLIGATIONS OF IEHP**

B. Notification of Restrictions to Use or Disclosure of PHI. IEHP agrees that it will make its best efforts to promptly notify Business Associate in writing of any restrictions, limitations, or changes on the use, access and disclosure of PHI and/or ePHI agreed to by IEHP in accordance with 42 U.S.C. § 17935(a), that may affect Business Associate's ability to perform its obligations under this Agreement.

C. Proper Use of PHI. IEHP shall not request Business Associate to use, access, or disclose PHI and/or ePHI in any manner that would not be permissible under the Privacy Rule, Security Rule, and/or HITECH.

D. Authorizations. IEHP will obtain any authorizations necessary for the use, access, or disclosure of PHI and/or ePHI, so that Business Associate can perform its obligations under this Agreement.

1. Actions in Response to Business Associate Breach. IEHP shall complete the following in the event that IEHP has determined that Business Associate has a Breach:

2. Determine appropriate method of notification to the patient/client(s) regarding a Breach as outlined in 45 C.F.R. § 164.404(d).

a. Send notification to the patient/client(s) without unreasonable delay but in no case later than sixty (60) days of Discovery of the Breach with at least the minimal required elements as follows:

b. Brief description of what happened, including the date of the Breach and the date of Discovery;

c. Description of the types of Unsecured PHI involved in the Breach (such as name, date of birth, home address, Social Security number, medical insurance, etc.);

d. Steps patient/client(s) should take to protect themselves from potential harm resulting from the Breach;

e. Brief description of what is being done to investigate the Breach, to mitigate harm to patient/client(s) and to protect against any further Breaches; and

3. Contact procedures for patient/client(s) to ask questions or learn additional information, which must include a toll-free telephone number, an E-Mail address, website or postal address.

4. Determine if notice is required to the Secretary and/or DHCS.

E. If required, submit Breach information to the Secretary within the required timeframe, in accordance with 45 C.F.R. § 164.408(b).

4. Contract Violations by Business Associate. Pursuant to 45 C.F.R. § 164.504(e)(1)(ii), if IEHP knows of a pattern of activity or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligations under this Agreement, IEHP must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, IEHP shall terminate the Agreement, if feasible.

A. **OBLIGATIONS OF BUSINESS ASSOCIATE**

B. Minimum Necessary. Business Associate shall request, use, access or disclose only the minimum amount of PHI and/or ePHI as permitted or required by this Agreement and as necessary to accomplish the intended purpose of the request, use, access or disclosure in accordance with the Privacy Rule (45 C.F.R. § 164.502(b)(1)).

1. Appropriate Safeguards. Business Associate shall use reasonable and appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI and/or ePHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical and technical safeguards in accordance with the Security Rule under 45 C.F.R. §§ 164.308, 164.310, 164.312 and

164.316 and be based on applicable Federal Information Processing Standards (FIPS) Publication 199 protection levels:

2. Business Associate shall issue and change procedures from time to time to improve electronic data and file security as needed to comply with the measures that may be required by the Privacy Rule or the Security Rule, as applicable, and at all times use an NIST-Approved Technology for all PHI and/or ePHI that is in motion, stored or to be destroyed.

C. Business Associate shall extend such policies and procedures, if applicable, for the protection of physical PHI to prevent, detect, contain and correct security violations, as well as to limit unauthorized physical access to the facility or facilities in which the PHI is housed.

D. Disclosure. Business Associate is solely responsible for its decisions regarding the safeguarding of PHI and other confidential information.

E. Mitigation. Business Associate shall have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use, access or disclosure of PHI and/or ePHI by Business Associate in violation of this Agreement.

F. Access to Records. Business Associate shall make facilities, internal practices, systems, books, and records including policies and procedures, relating to the use, access, disclosure, and privacy protection of PHI received from IEHP, or created or received by Business Associate on behalf of IEHP, available to the Secretary and/or DHCS, for purposes of determining, investigating or auditing Business Associate's, IEHP's, and/or DHCS' compliance with the Privacy and Security Rules and/or HITECH, subject to any applicable legal restrictions. Business Associate shall also cooperate with IEHP should IEHP elect to conduct its own such investigation and analysis.

G. Notification. If Business Associate is the subject of an audit, compliance review, investigation or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of HIPAA, Business Associate shall promptly notify IEHP unless it is legally prohibited from doing so.

H. Carrying Out IEHP's Obligations. To the extent Business Associate is to carry out one or more of IEHP's obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that applies to IEHP in the performance of such obligations.

I. Subcontractors. In accordance with 45 C.F.R. §§164.502(e)(1)(ii) and 164.308(b)(2), if applicable, Business Associate shall require Subcontractors that create, receive, maintain or transmit PHI and/or ePHI on behalf of Business Associate, to agree to the same restrictions, conditions and requirements that apply to Business Associate with respect to the PHI and/or ePHI, including the restrictions, conditions and requirements set forth in this Agreement.

J. Contract Violations by Subcontractors. Pursuant to 45 C.F.R. § 164.504(e)(1)(iii), if Business Associate knows of a pattern of activity or practice of the Subcontractor that constitutes a material breach or violation of the Subcontractor's obligations under the business associate contract between Business Associate and Subcontractor, Business Associate must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, Business Associate shall terminate the business associate contract with the Subcontractor if feasible.

K. Workforce Training. Business Associate warrants that all employees who use, access or disclose PHI and/or ePHI shall be properly trained to comply with Privacy Rule, Security Rule, HITECH, or other such applicable law.

L. Patient Confidentiality Laws and Regulations. Business Associate agrees to obtain and maintain knowledge of the applicable laws and regulations related to HIPAA and HITECH, as may be amended from time to time.

1. Reporting of Improper Access, Use or Disclosure Breach. Business Associate shall report to IEHP any unauthorized use, access or disclosure of Unsecured PHI and/or ePHI or any other Security Incident with respect to PHI no later than fifteen (15) days after Discovery of the potential Breach ("Notice Date"). With respect to PHI involving Medi-Cal beneficiaries, however, Business Associate shall report to IEHP any Breach or Security Incident of which Business Associate becomes aware, within 12 hours of discovery. Business Associate shall notify IEHP through the IEHP Compliance Department via telephone to the Compliance Hotline (866) 355-9038, via email to the Compliance Mailbox compliance@iehp.org, or via facsimile to the Compliance Fax (909) 477-8536. Upon Discovery of the potential Breach, Business Associate shall complete the following actions:

a. Provide IEHP's Compliance Department with the information required by 45 C.F.R. §§164.410 and 164.404, which shall include, but not be limited to:

b. The identification of each individual (IEHP Members) whose Unsecured PHI has been, or is reasonably believed by Business Associate, to have been accessed, acquired, used or disclosed;

c. Date(s) of Breach: MM/DD/YYYY;

d. Date(s) of Discovery of Breach: MM/DD/YYYY;

e. Approximate number of individuals (IEHP Members) affected by the Breach;

f. Type of Breach, i.e., theft, loss, improper disposal, unauthorized access, hacking/IT incident (for additional selections, see U.S. Department of Health & Human Services, Health Information Privacy);

g. Location of breached information, i.e., laptop, desktop computer, network server, E-Mail, other portable electronic device (see U.S. Department of Health & Human Services, Health Information Privacy);

h. Type of PHI involved in the Breach, i.e., demographic information, financial information, clinical information (see U.S. Department of Health & Human Services, Health Information Privacy);

i. Safeguards in place prior to Breach, i.e., firewalls, packet filtering (router-based), encrypted wireless (see U.S. Department of Health & Human Services, Health Information Privacy);

j. Actions taken in response to Breach, i.e., mitigation, protection against any further Breaches, policies and procedures (see U.S. Department of Health & Human Services, Health Information Privacy); and

2. Any steps individuals should take to protect themselves from potential harm resulting from the Breach.

a. Conduct and document a risk assessment by investigating, without unreasonable delay and in no case later than twenty (20) calendar days of Discovery, the potential Breach to determine the following:

b. Whether there has been an impermissible use, acquisition, access or disclosure of PHI and/or ePHI under the Privacy Rule;

c. Whether an impermissible use or disclosure compromises the security or privacy of the PHI and/or ePHI, including whether it can be demonstrated that there is a low probability that PHI and/or ePHI has been compromised based on a risk assessment of at least four (4) factors specified in Section 1.B(1) defining Breach; and

3. Whether the incident falls under one of the Breach exceptions.

a. Provide the completed risk assessment and investigation documentation to IEHP's Compliance Department within twenty-five (25) calendar days of Discovery of the potential Breach, and collaborate with IEHP on making a decision on whether a Breach has occurred.

b. If a Breach has not occurred, notification to patient/client(s) is not required;

4. If a Breach has occurred, notification to the patient/client(s) is required and Business Associate must provide IEHP with affected patient/client(s) names and contact information so that IEHP can provide notification.

5. For Breaches or Security Incidents involving Medi-Cal PHI, Business Associate shall commence investigations immediately and work with IEHP to submit a "DHCS Privacy Incident Report" within 72 hours of discovery with the information known at the time. Within ten (10) working days of the discovery of the Breach or unauthorized use or disclosure, Business Associate shall work with IEHP to provide a complete report of the investigation to DHCS, which shall include (i) an assessment of all known factors relevant to a determination of whether a Breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law; and (ii) a corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests additional information to that listed on the "DHCS Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide DHCS with such information.

6. Make available to governing State and Federal agencies in a time and manner designated by such agencies, any policies, procedures, internal practices and records relating to a potential Breach for the purposes of audit; cooperate with IEHP should IEHP elect to conduct its own such investigation and analysis.

7. Should the Breach of Unsecured PHI be caused solely by Business Associate's failure to comply with one or more of its obligations under this BAA, Privacy Rule, Security Rule and/or HITECH Provisions, Business Associate shall pay for any and all costs associated with providing all legally required notifications to individuals, media outlets and the Secretary.

8. Should the Breach of Unsecured PHI involve more than 500 residents of a single State or jurisdiction, Business Associate shall provide to IEHP, no later than the Notice Date, the information necessary for IEHP to prepare the notice to media outlets as set forth in 45 C.F.R. § 164.406.

9. Should the Breach of Unsecured PHI involve 500 or more individuals, Business Associate shall provide to IEHP, no later than the Notice Date, the information necessary for IEHP to prepare the notice to the Secretary as set forth in 45 C.F.R. § 164.408.

M. Should the Breach of Unsecured PHI involve less than 500 individuals, Business Associate shall maintain a log of such Breaches and provide such log to IEHP, for submission to the Secretary, on an annual basis and not later than forty-five (45) days after the end of each calendar year.

N. Monitoring. Business Associate shall comply with all monitoring provisions of this Agreement and any monitoring requests by DHCS.

1. General Security Controls.

2. Confidentiality Statement. All persons that will be working with DHCS PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.

3. Background Check. Before a member of the workforce may access DHCS PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

4. Transmission and Storage. The most current industry standards for transmission and storage of PHI and other confidential information must be used.

5. Workstation/Laptop encryption. All workstations and laptops that process and/or store DHCS PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.

6. Minimum Necessary. Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

7. Removable media devices. All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

8. Email Security. All emails that include DHCS PHI must be sent in a FIPS 140-2 compliant encryption method using a DHCS approved solution or a solution using a vendor product specific on the CSSI.

9. Antivirus software. All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution from a commercial third-party with automatic updates scheduled at least daily.

10. Patch Management. All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

a. User IDs and Password Controls. All users must be issued a unique user name for accessing DHCS PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days.

Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

b. Upper case letters (A-Z)

c. Lower case letters (a-z)

d. Arabic numerals (0-9)

11. Non- alphanumeric characters (punctuation symbols)

12. Data Destruction. When no longer needed, all DHCS PHI or PI must be wiped using the Gutmann or US Department of Defense (DOD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the DHCS Information Security Office.

O. Remote Access. Any remote access to DHCS PHI must be executed over an encrypted method approved by DHCS or using a vendor produce specified on the CSSI. All remote access must be limited to minimum necessary and least privilege principles.

1. <u>System Security Controls.</u>

2. System Timeout. The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

3. Warning Banners. All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

4. System Logging. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

5. Access Controls. The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

6. Transmission encryption. All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

P. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

1. Audit Controls.

2. System Security Review. All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

3. Log Reviews. All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access. Logs must be maintained for six years after the occurrence.

Q. Change Control. All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

1. Business Continuity/Disaster Recovery Controls.

2. Emergency Mode Operation Plan. Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

R. Data Backup Plan. Contractor must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

1. Paper Document Controls.

2. Supervision of Data. DHCS PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

3. Escorting Visitors. Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

4. Confidential Destruction. DHCS PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

5. Removal of Data. DHCS PHI or PI must not be removed from the premises of the Contractor except with express written permission of DHCS.

6. Faxing. Faxes containing DHCS PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

5. Mailing. Mailings of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained Disks and other transportable media sent through the mail must be encrypted.

A. **ACCESS TO PHI, AMENDMENT AND DISCLOSURE ACCOUNTING**

Business Associate agrees to:

B. Provide access, at the request of IEHP, within five (5) days, to PHI, including ePHI if maintained electronically, in a Designated Record Set, to IEHP, or to an individual or individual's designee as directed by IEHP, as necessary for IEHP to satisfy its obligations under 45 C.F.R. § 164.524.

C. Make any amendment(s) to PHI in a Designated Record Set that IEHP directs or agrees to, at the request of IEHP or an individual, pursuant to 45 C.F.R. § 164.526, within thirty (30) days of the request of IEHP.

1. Assist IEHP in meeting its disclosure accounting under HIPAA:

2. Business Associate agrees to document such disclosures of PHI and information related to such disclosures, as would be required for IEHP to respond to a request by an individual for an accounting of disclosures of PHI.

3. Business Associate agrees to provide to IEHP, within thirty (30) days,

information collected in accordance with this Section to permit IEHP to make an accounting of disclosures of PHI by Business Associate in accordance with 45 C.F.R. § 164.528 and HITECH.

6. Business Associate shall have available for IEHP the information required by this Section for the six (6) years preceding IEHP's request for information.

A. **TERM AND TERMINATION**

B. Term. This Agreement shall commence upon the Effective Date and terminate on ***<insert Date of Termination>*** ("Termination Date") unless sooner terminated in accordance with the terms and conditions of this Agreement.

1. Termination for Cause. IEHP may terminate this Agreement, effective immediately, if IEHP, in its sole discretion, determines that Business Associate has breached a material provision of this Agreement relating to the privacy and/or security of the PHI. Alternatively, IEHP may

choose to provide Business Associate with notice of the existence of an alleged material breach and afford Business Associate with an opportunity to cure the alleged material breach. In the event Business Associate fails to cure the breach to the satisfaction of IEHP in a timely manner, IEHP reserves the right to immediately terminate this Agreement.

2. Effect of Termination. Upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI and/or ePHI received from IEHP, or created or received by Business Associate on behalf of IEHP, no later than sixty (60) days after the date of termination. Business Associate shall certify such destruction, in writing, to IEHP. This provision shall apply to all PHI and/or ePHI which is in possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI and/or ePHI.

7. Destruction not Feasible. In the event that Business Associate determines that returning or destroying the PHI and/or ePHI is not feasible, Business Associate shall provide written notification to IEHP of the conditions which make such return or destruction not feasible. Upon determination by Business Associate that return or destruction of PHI and/or ePHI is not feasible, Business Associate shall extend the protections, limitations, and restrictions of this Agreement to such PHI and/or ePHI retained by Business Associate, its subcontractors, employees or agents, and to limit further uses and disclosures of such PHI and/or ePHI to those purposes which make the return or destruction not feasible, for so long as such PHI and/or ePHI is maintained.

8. HOLD HARMLESS/INDEMNIFICATION

Business Associate shall indemnify and hold harmless IEHP, its respective directors, officers, Governing Board, employees, agents and representatives from any liability whatsoever, based or asserted upon any services of Business Associate, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Agreement, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature whatsoever including fines, penalties or any other costs and resulting from any reason whatsoever arising from the performance of Business Associate, its officers, agents, employees, subcontractors, agents or representatives from this Agreement. Business Associate shall defend, at its sole expense, all costs and fees including but not limited to attorney fees, cost of investigation, defense and settlements or awards IEHP, its respective directors, officers, Governing Board, elected and appointed officials, employees, agents and representatives in any claim or action based upon such alleged acts or omissions.

With respect to any action or claim subject to indemnification herein by Business Associate, Business Associate shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of IEHP, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of IEHP; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Business Associate's indemnification to IEHP as set forth herein. Business Associate's obligation to defend, indemnify and hold harmless IEHP shall be subject to IEHP having given Business Associate written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at Business Associate's expense, for the defense or settlement thereof. Business Associate's obligation hereunder shall be satisfied when Business Associate has provided to IEHP the appropriate form of dismissal relieving IEHP from any liability for the action or claim involved.

A. **GENERAL PROVISIONS**

B. Medi-Cal Requirements. As a condition of obtaining access to PHI of IEHP relating to Medi-Cal Members, Business Associate acknowledges receipt of a copy of Exhibit G of the contract between IEHP and DHCS (which can also be found at: https://www.dhcs.ca.gov/provgovpart/Documents/Two-PlanCCIFinalRuleBoilerplate.pdf), and agrees to the terms and conditions therein with respect to such PHI.

C. Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for IEHP to comply with the Privacy Rule, Security Rule, HITECH, and HIPAA generally.

D. Survival. Notwithstanding Section 6.A of this Agreement, the respective rights and obligations of this Agreement shall survive the termination or expiration of this Agreement.

E. Regulatory References. A reference in this Agreement to a section in the Privacy Rule, Security Rule, and/or HITECH means the section(s) as in effect or as amended.

F. Interpretation. Any ambiguity in this Agreement shall be resolved to permit IEHP to comply with the Privacy Rule, Security Rule, HITECH, and HIPAA generally.

G. Remedies. Business Associate agrees that IEHP shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which IEHP may have at law or in equity in the event of an

unauthorized use, access, or disclosure of PHI by Business Associate or any agent or subcontractor of Business Associate that received PHI from Business Associate.

H. No Third-Party Beneficiaries. Nothing in this Agreement is intended to or shall confer, upon any third person any rights or remedies whatsoever.

I. Ownership. The PHI shall be and remain the property of IEHP. Business Associate agrees that it acquires no title or rights to the PHI.

J. Headings. Paragraph headings contained in this Agreement are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this Agreement.

K. Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself and its employees and use all due diligence to make any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.