DATA USE AGREEMENT

BETWEEN

INLAND EMPIRE HEALTH PLAN

AND

HOUSING AUTHORITY OF THE COUNTY OF SAN BERNARDINO

AND

SAN BERNARDINO COUNTY

AND

VALLEY STAR BEHAVIORAL HEALTH, INC.

AND

STEP UP ON SECOND STREET, INC.

AND

INLAND HOUSING SOLUTIONS

FOR

DESERT HAVEN APARTMENTS

This Data Use Agreement ("Agreement") is made effective upon execution (March 24, 2026) by and between Inland Empire Health Plan ("IEHP" or "Covered Entity"), a local public entity of the State of California and Housing Authority of the County of San Bernardino, San Bernardino County Department of Behavioral Health, Valley Star Behavioral Health, Inc., Step Up on Second Street, Inc., and Inland Housing Solutions (collectively, "Recipient"). Either party may be referred to individually as the "Party" or collectively as "the Parties."

WHEREAS, IEHP possesses certain data, including Protected Health Information (PHI) and/or electronic Protected Health Information (ePHI) as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), and desires to share such data with Recipient(s) for the purpose providing housing units, intensive case management, and community health services for qualified IEHP Members at Desert Haven Apartments (the "Project"); and

WHEREAS, the Parties recognize the importance of protecting the privacy and security of the data to be shared, and wish to comply with all applicable federal, state, and local laws and

regulations, including but not limited to HIPAA, the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (45 CFR Parts 160 and 164), the California Confidentiality of Medical Information Act ("CMIA"), and any other applicable privacy laws;

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

1. Definitions. Unless otherwise specified in this Agreement, all capitalized terms have the same meanings as set forth in the HIPAA Regulations, as amended from time to time.

2. Responsibilities of Recipient. Recipient agrees to:

    a. Not use or further disclose the PHI or ePHI other than as permitted by this Agreement or as otherwise required by law;
    b. Use appropriate safeguards to prevent use or disclosure of the information in the PHI or ePHI other than as provided for by this Agreement;
    c. Report to IEHP any use or disclosure of the information in the PHI or ePHI not provided for by this Agreement of which it becomes aware;
    d. Ensure that any agents or subcontractors to whom it provides the PHI or ePHI agree to the same restrictions and conditions that apply to Recipient with respect to such information; and
    e. Comply with all applicable requirements of HIPPA and abide by the terms of the Business Associate Agreement ("BAA") attached hereto as Attachment A and incorporated herein by reference, to the extent Recipient is acting as a Business Associate of IEHP, a Covered Entity under HIPAA.
    f. Comply with all relevant Federal and State laws and regulations, including, but not limited to those listed below, inclusive of future revisions, and comply with all applicable provisions of:
        i. Welfare and Institution Code 5328 et seq.,
        ii. Welfare and Institution Code 14100.2,
        iii. Title 22, California Code of Regulations Section 51009, and
        iv. Code of Federal Regulations, Title 42, Part 2.

3. Permitted Uses and Disclosures of the PHI or ePHI.

    a. Except as otherwise specified herein, Recipient may use and/or disclose the PHI or ePHI necessary for the Project or as required by law.
    b. Recipient shall receive or have access to only the following types of confidential PHI or ePHI from IEHP:
        i. Identifying information on all active IEHP Members living at Desert Haven Apartments, including Member ID numbers, names, and dates of birth.
        ii. Select information from Member health records subject to IEHP approval, including Member Primary Care Physicians ("PCP"), open referrals, prior utilization data, and prescription medications.

c. Recipient understands that this Agreement does not authorize the Recipient to have greater rights to use or disclose the information than that which is granted to IEHP pursuant to the HIPAA Regulations.

d. Recipient has designated the following individual(s) and/or classes of individuals, who are permitted to use or receive the PHI or ePHI for purposes of the Project: ***Interdisciplinary Care Team providing case management to individuals housed at Desert Haven Apartments.*** To the extent the classes of individuals are not part of Recipient's workforce who are directly involved in the Project, Recipient shall enter into a data use agreement, including the attached Business Associate Agreement, that complies with the HIPAA Regulations, prior to the release of the PHI or ePHI with the other classes of individuals.

e. Recipient shall use the above described PHI or ePHI for purposes of the Project only.

4. Term and Termination.

a. Term. The term of this Agreement shall commence as of March 24, 2026, and terminate on October 31, 2030. Upon termination of this Agreement, Recipient(s) agrees to immediately furnish to IEHP all data, including PHI and ePHI, received under this Agreement.

b. Termination for Convenience. Either Party may terminate this Agreement, for convenience upon thirty (30) days' written notice.

c. Termination for Breach. Upon IEHP's knowledge of a pattern or practice that constitutes a material breach of this Agreement by Recipient, IEHP may immediately and unilaterally terminate this Agreement. Alternatively, IEHP may provide an opportunity for Recipient to cure the breach or end the violation. If such efforts are not successful within the reasonable time period specified by IEHP, or if IEHP determines that cure of the breach is not possible, IEHP shall immediately discontinue disclosure of the PHI or ePHI to Recipient and report the problem to the Secretary of the Department of Health and Human Services or its designee.

5. Indemnification. Each Party agrees to indemnify, defend (with counsel approved by the other Party) and hold harmless the other Parties ("Indemnitees") and their authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages, and/or liability arising out of this Agreement, but only to the extent actually caused by the negligent acts, errors or omissions of the indemnifying Party and its authorized officers, employees, agents, and volunteers, and for any costs or expenses incurred by Indemnitees on account of any claim except where such indemnification is prohibited by law.

   If the Parties are determined to be comparatively at fault for any claim, action, loss, or damage which results from their respective obligations under this Agreement, each Party shall indemnify the others to the extent of its comparative fault as determined in a legal action.

6. Insurance. Each Party is an authorized self-insured or partially self-insured public entities for purposes of Professional Liability, General Liability, Automobile Liability and Worker's Compensation and warrant that through their respective programs of self-insurance and

insurance, they have adequate coverage or resources to protect against liabilities arising out of performance of the terms, conditions or obligations of this Agreement.

7. Notice. All correspondence and notices required or contemplated by this Agreement shall be delivered at the addresses set forth below, and are deemed submitted two (2) days after their deposit in the United States mail, postage prepaid:

IEHP
Edward Juhn, MD, MBA, MPH
Chief Medical Officer for
Jarrod McNaughton, MBA, FACHE
Chief Executive Officer
IEHP
10801 Sixth Street
Rancho Cucamonga, CA 91730
(909) 890-2000
Juhn-E@iehp.org

INLAND HOUSING SOLUTIONS
Jeff Little
CEO
Inland Housing Solutions
P.O. Box 239
Loma Linda, CA 92354
(909) 796-6381, ext. 106
jeff@inlandhousingsolutions.org

HOUSING AUTHORITY OF THE COUNTY OF SAN BERNARDINO:
Maria Razo
Executive Director
Housing Authority of the County of San Bernardino
715 East Brier Drive
San Bernardino, CA 92408
(909) 890-0644
mgrazo@hacsb.com

SAN BERNARDINO COUNTY DEPARTMENT OF BEHAVIORAL HEALTH:
Joshua Dugas, Acting Director
San Bernardino County Department of Behavioral Health:
550 Hospitality Lane Vanderbilt Way
San Bernardino, CA 92415
(909) 252-5142
Joshua.Dugas@dbh.sbcounty.gov

VALLEY STAR BEHAVIORAL HEALTH:
Robert Lopez, LCSW
Senior Administrator
Valley Star Behavioral Health
12188 Hesperia
Victorville, CA 92395
(760) 477-2199
roblopez@starsinc.com

STEP UP ON SECOND STREET, INC.
Tod Lipka
President and CEO
Step Up on Second Street, Inc.
1329 2nd Street
Santa Monica, CA 90401
(310) 394-6883
tlipka@stepup.org

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

8. General Provisions.

a. Construction of Terms. The terms of this Agreement shall be construed to give effect to applicable federal interpretative guidance regarding the HIPAA Regulations. A reference in this Agreement to a section in the HIPAA Regulations means the section(s) as in effect or as amended.

b. No Third-Party Beneficiaries. Nothing in this Agreement shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

c. Independent Contractors. The Parties are independent contractors. Neither Party has the power or authority to act on behalf of the other Party as its agent. Nothing in this Agreement shall be construed to make the Parties hereto partners, joint venturers, or agents of or with each other, nor shall either Party so represent itself.

d. Amendment. This Agreement shall not be amended or assigned by either Party without the prior written consent of the other. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the Parties to comply with HIPAA Regulations.

e. Law and Venue. This Agreement shall be governed by the laws of California, without regard to its principles of conflicts of law. All actions and proceedings arising in connection with this Agreement shall be tried and litigated exclusively in the state or federal courts located in the counties of San Bernardino or Riverside, State of California.

f. Entire Agreement/Severability. This Agreement constitutes the entire agreement between IEHP and Recipient, and supersedes all other prior and contemporaneous agreements, understandings, and commitments between them, relating to the subject matter hereof. The invalidity of any provision of this Agreement shall not affect the validity of the remaining provisions, and this Agreement shall be construed as if such invalid provision had been omitted.

g. Expense of Performance. Each Party shall bear its own expenses as to the sharing of data unless otherwise specified in this Agreement.

h. Survival. Unless otherwise provided herein, the rights and obligations of any Party which by their nature extend beyond the expiration or termination of this Agreement, shall continue in full force and effect, notwithstanding the expiration or termination of this Agreement.

i. Remedies. IEHP shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies IEHP may have at law or in equity in the event of an unauthorized use, access, or disclosure of the PHI or ePHI by Recipient or any agent or subcontractor of Recipient that received information from Recipient. Recipient hereby waives any requirement that IEHP post any bond or other security in the event any injunctive or equitable relief is sought by IEHP.

j. Ownership. The PHI or ePHI shall be and remain the property of IEHP. Recipient agrees that it acquires no title or rights to the PHI or ePHI.

k. Public Statements; Publicity; Publications; Work Product; Intellectual Property.

i. Publicity and Public Statements. Without IEHP's prior written consent, Recipient shall not issue any press release, public announcement, marketing, promotional, or social media communication; publish, present, disseminate, or otherwise publicly disclose any information concerning this Agreement, the Parties' relationship, the Project or Services, any data shared or compiled under this Agreement, or analyses, results, or outcomes generated hereunder (including any pilot, proof-of-concept, or evaluation results); and shall not use or display IEHP's name, trade name, trademarks, service marks, logos, or other identifiers, or refer to IEHP as a client, partner, or reference. Recipient shall submit any permitted disclosure to IEHP for review and written approval at least thirty (30) days in advance, and IEHP may require edits, redactions, or disclaimers as a condition of approval. If Recipient is legally required to make a public disclosure, Recipient shall, to the extent lawful, provide IEHP with prompt prior written notice and reasonably cooperate to limit the disclosure and seek confidential treatment. Recipient may disclose on a need-to-know basis to its affiliates, professional advisors, and potential investors, lenders, or acquirers under written confidentiality obligations no less protective than those herein. Nothing in this Section grants any license or publicity rights in IEHP's name or marks. This Section supplements the Parties' confidentiality obligations and survives expiration or termination. IEHP shall be entitled to injunctive relief for any actual or threatened breach of this Section, without the requirement to post bond.

ii. Publications and Academic/Program Evaluations. Recipient shall not publish or present any report, paper, poster, presentation, or other publication based on data, information, or work product shared or compiled under this Agreement without IEHP's prior written consent. Any permitted publication shall comply with HIPAA, CMIA, 42 C.F.R. Part 2, and other applicable privacy laws; use only de-identified information unless otherwise expressly authorized; and include disclaimers requested by IEHP. This subsection does not restrict disclosures required by law, including the California Public Records Act (CPRA), provided that Recipient complies with subsection A and uses reasonable efforts to notify IEHP and seek confidential treatment to the extent permitted.

iii. Work Product and Ownership. All work product created by Recipient under or in connection with this Agreement on behalf of IEHP—including reports, findings, analyses, documents, compilations, aggregated datasets, and derivative works of IEHP Data—shall be IEHP's property and, upon expiration or termination, shall be transmitted to IEHP in accordance with this Agreement. Ownership of PHI/ePHI remains as set forth elsewhere in this Agreement.

iv. Background and Embedded Intellectual Property. As between the Parties, no Party assigns or transfers ownership of pre-existing intellectual property, methodologies, processes, know-how, templates, tools, or models

("Background IP"). To the extent any Recipient Background IP is contained in any data, information, or work product shared or compiled under this Agreement, Recipient grants IEHP a paid-up, royalty-free, nonexclusive, perpetual license to use and reproduce such Recipient Background IP solely for IEHP's internal business operations in connection with the Project. Nothing herein grants Recipient any license, right, or interest in IEHP's name, trademarks, or other intellectual property.

v. Survival. The obligations in this Section survive expiration or termination of this Agreement.

l. 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.

m. Counterparts/Signatures. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. The Parties' faxed signatures, and/or signatures scanned into PDF format, shall be effective to bind them to this Agreement.

n. Authority. The Parties certify that the individuals signing below have the proper authority to execute this Agreement on behalf of the Parties.

[SIGNATURE PAGE TO FOLLOW]

IN WITNESS WHEREOF, the Parties hereby execute this Agreement.

SAN BERNARDINO COUNTY

►

Dawn Rowe, Chair, Board of Supervisors

Dated: _____

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD

Lynna Monell
Clerk of the Board of Supervisors
San Bernardino County

By _____
Deputy

Inland Empire Health Plan
(Print or type name of corporation, company, contractor, etc.)

By ►
(Authorized signature - sign in blue ink)

Name Edward Juhn, MD, MBA, MPH for: Jarrod McNaughton, MBA FACHE
(*Print or type name of person signing contract)*

Title Chief Medical Officer for Chief Executive Officer
(Print or Type)

Dated: _____

Address 10801 Sixth Street

Rancho Cucamonga, CA 91730

By: _____
Chair, IEHP Governing Board

Date: _____

Approved as to form:

Attest: _____
Secretary, IEHP Governing Board

By:_____
Anna W. Wang
Vice President, General Counsel
Inland Empire Health Plan

Date:_____

Date: _____

HOUSING AUTHORITY OF THE COUNTY OF SAN BERNARDINO:

By: _____
Maria Razo
Executive Director

Date: _____

INLAND HOUSING SOLUTIONS

By: _____
Jeff Little
CEO

Date: _____

VALLEY STAR BEHAVIORAL HEALTH:

By:_____
Robert Lopez, LCSW
Senior Administrator

Date: _____

STEP UP ON SECOND STREET, INC.

By: _____
Tod Lipka,
President and CEO

Date: _____

ATTACHMENT A

HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement (the "Agreement") is an Attachment to the Data Use Agreement (the "Underlying Agreement") between the Inland Empire Health Plan ("IEHP") and Housing Authority of the County of San Bernardino, San Bernardino County Department of Behavioral Health, Valley Star Behavioral Health, Step Up on Second Street, Inc., Inland Housing Solutions, and Desert Haven Apartments ("Business Associate") as of the "Effective Date," of the Underlying Agreement.

RECITALS

WHEREAS, IEHP and Business Associate entered into the Underlying 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 Underlying 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 the Underlying 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;

WHEREAS, IEHP, is in contract with Covered California to participate as a Qualified Health Plan ("QHP") on the California Health Benefit Exchange ("Covered California");

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

1. DEFINITIONS

A. 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.

B. Specific Definitions:

(1) "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:

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

b) The unauthorized person who used the PHI or to whom the disclosure was made;

c) Whether the PHI was actually acquired or viewed; and

d) The extent to which the risk to PHI has been mitigated.

(2) "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.

(3) "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.

(4) "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.

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

(6) "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.

(7) "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).

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

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

1) 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.

2) As necessary to perform any and all of its obligations under the Underlying Agreement.

B. 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:

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

2) 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:

i. The disclosure is required by law; or

ii. 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:

a) 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

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

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

4) 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.

C. Business Associate shall not:

1) 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.

2) 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.

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

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

5) Use or disclose PHI for fundraising or marketing purposes.

6) 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)).

7) 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 the Underlying Agreement.

8) 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.

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

D. 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. The Business Associate will treat any violation of such additional protective standards as a breach or security incident. 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. Business Associate agrees to comply with all applicable California state health information privacy and security laws, including the Confidentiality of Medical Information Act, the California Insurance Information and Privacy Protection Act, and the Information Practices Act.

E. 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.

3. OBLIGATIONS OF IEHP

A. 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 the Underlying Agreement, or this Agreement.

B. 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.

C. 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 and/or the Underlying Agreement.

D. 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:

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

(2) 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:

a) Brief description of what happened, including the date of the Breach and the date of Discovery;

b) 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.);

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

d) 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

e) 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.

(3) Determine if notice is required to the Secretary and/or DHCS. This notification will be provided by email upon discovery of the breach. If IEHP is unable to provide notification by email, then IEHP shall provide notice by telephone to DHCS.

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

E. 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.

F. Identification of Security Official: The Business Associate shall identify the security official who is responsible for the development and implementation of the policies and procedures required by 45 CFR Part 164, Subpart C.

4. OBLIGATIONS OF BUSINESS ASSOCIATE

A. 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)).

B. 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:

(1) 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.

(2) 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.

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

D. 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.

E. 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.

F. 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

G. 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.

H. In conducting any electronic transaction that is subject to the Electronic Transactions Rule on behalf of IEHP, Business Associate agrees to comply with all applicable requirements of the Electronic Transactions Rule set forth in 45 CFR. Part 162.

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 workforce members including employees, contractors, temporary staff, volunteers, and interns/students 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. Training must be conducted prior to access is granted to PHI and annually thereafter, and include at minimum:
(1) Definitions of PHI and PII
(2) Use and disclosures for PHI
(3) How to report privacy concerns/breaches
(4) Best practices for safeguarding PHI
(5) Enforcement of policies and procedures

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.

M. 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 24 hours after Discovery of the potential Breach ("Notice Date"). With respect to PHI involving Medi-Cal beneficiaries, SSA data, or potential loss of confidential data affecting this Agreement, Business Associate shall report to IEHP any Breach or Security Incident of which Business Associate becomes aware, within 24 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:

(1) 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:

a) 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;

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

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

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

e) 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);

f) 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);

g) 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);

h) 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);

i) 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

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

(2) Conduct and document a risk assessment by investigating, without unreasonable delay and in no case later than five (5) calendar days of Discovery, the potential Breach to determine the following:

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

b) 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

c) Whether the incident falls under one of the Breach exceptions.

(3) Provide the completed risk assessment and investigation documentation to IEHP's Compliance Department within seven (7) calendar days of Discovery of the potential Breach, and collaborate with IEHP on making a decision on whether a Breach has occurred.

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

ii. 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.

(4) 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.

(5) For Breaches or Security Incidents involving Covered California PHI/PII, Business Associate shall cooperate with Covered California and IEHP in investigating the Breach and/or successful Security Incident involving PHI and/or Personally Identifiable Information and in meeting Covered California's obligations, if any, under applicable State and federal security breach notification laws, regulatory obligations, or agency requirements. If the cause of the Breach or the successful Security Incident involving PHI and/or Personally Identifiable Information is attributable to Business Associate, Business Associate shall be responsible for Breach notifications and reporting as required under applicable federal and State laws, regulations, and agency guidance. Such notification(s) and required reporting shall be done in cooperation with Covered California and IEHP.

(6) Make available to IEHP or 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.

(10) 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. Business Associate shall implement policies and procedures to conduct routine auditing and monitoring of its systems and controls to monitor safeguards implemented to protect PHI are effective.

O. Audit Rights. Business Associate shall comply with auditing and/or monitoring requests issued by IEHP. 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 IEHP, for purposes of determining, investigating or auditing Business Associate's, IEHP's, and/or IEHP's regulatory agencies compliance with the Privacy and Security Rules and/or HITECH, subject to any applicable legal restrictions.

P. General Security Controls.

(1) 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 ten (10) years following contract termination.

(2) 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.

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

(4) 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.

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

(6) 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.

(7) 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.

(8) 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.

(9) 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.

(10) 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. Business Associate shall immediately notify IEHP via e-mail through an e-mail address provided by IEHP once any such employees, sub-contractors, agents or other such individuals are no longer employed or retained by Business Associate. 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:

a) Upper case letters (A-Z)

b) Lower case letters (a-z)

c) Arabic numerals (0-9)

d) Non- alphanumeric characters (punctuation symbols)

(11) 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.

(12) 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.

(13) Incident Response Plan. Develop an incident plan which can be exercised and implemented to respond to internal and external security threats and violations.

Q. System Security Controls.

(1) 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.

(2) 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.

(3) 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.

(4) 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.

(5) 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.

(6) 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.

R. Audit Controls.

(1) 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.

(2) 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 ten (10) years after the occurrence.

(3) 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.

S. Business Continuity/Disaster Recovery Controls.

(1) 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.

(2) 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.

T. Paper Document Controls.

(1) 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.

(2) 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.

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

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

(5) 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.

(6) 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.

5. ACCESS TO PHI, AMENDMENT AND DISCLOSURE ACCOUNTING

Business Associate agrees to:

A. 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.

B. 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.

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

1) 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.

2) 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.

3) Business Associate shall have available for IEHP the information required by this Section for the ten (10) years preceding IEHP's request for information.

6. TERM AND TERMINATION

A. Term. This Agreement shall commence upon the Effective Date and terminate upon the termination of the Underlying Agreement.

B. Termination for Cause. IEHP may terminate the Underlying 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 the Underlying Agreement.

(1) Effect of Termination. Upon termination of the Underlying 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.

(2) 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.

7. HOLD HARMLESS/INDEMNIFICATION

With respect to the subject matter in this Agreement, the following shall be applicable:

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.

With respect to a Breach or other non-permitted use of disclosure of PHI or PII of a Covered California member by Business Associate, Business Associate shall additionally indemnify, hold harmless, and defend Covered California from and against any and all costs (including mailing, labor, administrative costs, vendor charges, and any other costs Covered California determines to be reasonable), losses, penalties, fines, and liabilities arising from or due to a Breach or other non-permitted use or disclosure of PHI and/or Personally Identifiable Information by Business Associate or its Subcontractors or agents, including, without limitation, (1) damages resulting from any action under applicable (a) HIPAA Requirements, (b) the Qualified Health Plan Contract requirements, or (c) California law, and (2) the costs of Covered California's actions taken to: (a) notify the affected Individual(s) and other entities of and to respond to the Breach; (b) mitigate harm to the affected Individual(s); and (c) respond to questions or requests for information about the Breach or other impermissible use or disclosure of PHI and/or Personally Identifiable Information.

The specified insurance limits required in the Underlying Agreement shall in no way limit or circumscribe Business Associate's obligations to indemnify and hold harmless IEHP herein from third party claims arising from the issues of this Agreement.

In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement, this indemnification shall only apply to the subject issues included within this Agreement.

8. GENERAL PROVISIONS

A. 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-Plan-CCI-Final-Rule-Boilerplate.pdf), and agrees to the terms and conditions therein with respect to such PHI.

B. 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.

C. 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.

D. 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.

E. Interpretation. This Attachment shall be construed to be a part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of HIPAA and HITECH. Any ambiguity in this Agreement and the Underlying Agreement shall be resolved to permit IEHP to comply with the Privacy Rule, Security Rule, HITECH, and HIPAA generally.

F. 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.

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

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

I. 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.

J. 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.