KAISER PERMANENTE

MEDI-CAL HIPAA FLOW-DOWN REQUIREMENTS FOR VENDORS, CONTRACTORS AND SUPPLIERS

Kaiser Foundation Health Plan, Inc., as a Medicaid managed care contractor of the California Department of Health Care Services, is required to flow-down the attached California Department of Health Care Services ("DHCS") HIPAA Requirements to Suppliers that create, receive, maintain, transmit, use or disclose Medi-Cal Member Information. Kaiser Foundation Hospitals may procure goods/services for the benefit of Kaiser Foundation Health Plan, Inc., and in such cases, is also required to flow-down the attached Medi-Cal HIPAA Flow-Down Requirements.

1. DEFINITIONS.

Capitalized terms used but not otherwise defined in these Medi-Cal HIPAA Flow-Down Requirements shall have the meanings provided in the Contract or associated Business Associate Agreement ("BAA"). The following definitions shall apply for purposes of these Medi-Cal Flow-Down Requirements only.

1.1. "Business Associate" and "Contractor" mean KP.

1.2. "Contract" means the written agreement between KP and Supplier.

1.3. "KP" means Kaiser Foundation Health Plan, Inc. and Kaiser Foundation Hospitals.

1.4. "Medi-Cal Member Information" means any Protected Health Information or Personal Information (as defined in Exhibit A hereto) of individuals enrolled in a KP Medi-Cal managed care plan in California.

1.5. "Supplier" means a vendor, contractor or supplier providing services to KP.

2. REQUIREMENTS.

If Supplier creates, receives, maintains, transmits, uses or discloses Medi-Cal Member Information, the following shall apply:

2.1. Supplier will comply with the applicable provisions of Exhibit A, attached hereto, which incorporates Exhibit G (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)) of the DHCS Medi-Cal managed care plan agreements with Kaiser Foundation Health Plan, Inc., a KP Entity (the "DHCS HIPAA Requirements"), provided that under the DHCS HIPAA Requirements: (a) KP is the "Contractor" and "Business Associate" referenced therein; and (b) Supplier's obligations are owed only to KP.

2.2. Notwithstanding any other provisions in the Contract or associated BAA, Supplier shall notify KP (a) immediately by telephone call, plus email or fax, upon the discovery of a Breach of Unsecured Protected Health Information or of any access, Use or Disclosure of PHI that is in violation of the BAA, and (b) within 24 hours by email or fax of the discovery of any suspected Security Incident, intrusion or unauthorized access, Use or Disclosure of PHI in violation of the BAA. Capitalized terms in this Section 2 have the meanings provided in the BAA. The contact information for notifications shall be as provided in the BAA.

These Medi-Cal HIPAA Flow-Down Requirements apply in addition to the provisions in the Contract and BAA.

KAISER PERMANENTE

EXHIBIT A

Exhibit G – HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) of the DHCS Medi-Cal managed care plan agreements with Kaiser Foundation Health Plan, Inc., a KP Entity, which is required to flow down Exhibit G - HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) to any Supplier who creates, receives, maintains, transmits, uses or discloses Medi - Cal Member Information.

Kaiser Foundation Health Plan, Inc.
23-30231
Exhibit G

Exhibit G – Business Associate Addendum

1. This Agreement has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act (HIPAA) and its implementing privacy and security regulations at 45 Code of Federal Regulations parts 160 and 164 (collectively, and as used in this Agreement)

2. The term "Agreement" as used in this document refers to and includes both this Business Associate Addendum and the contract to which this Business Associate Agreement is attached as an exhibit, if any.

3. For purposes of this Agreement, the term "Business Associate" shall have the same meaning as set forth in 45 CFR section 160.103.

4. The Department of Health Care Services (DHCS) intends that Business Associate may create, receive, maintain, transmit or aggregate certain information pursuant to the terms of this Agreement, some of which information may constitute Protected Health Information (PHI) and/or confidential information protected by federal and/or State laws.

   4.1 As used in this Agreement and unless otherwise stated, the term "PHI" refers to and includes both "PHI" as defined at 45 CFR section 160.103 and Personal Information (PI) as defined in the Information Practices Act (IPA) at California Civil Code section 1798.3(a). PHI includes information in any form, including paper, oral, and electronic.

   4.2 As used in this Agreement, the term "confidential information" refers to information not otherwise defined as PHI in Section 4.1 of this Agreement, but to which State and/or federal privacy and/or security protections apply.

5. Contractor (however named elsewhere in this Agreement) is the Business Associate of DHCS acting on DHCS' behalf and 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 (collectively, "use or disclose PHI") in order to fulfill Business Associate's obligations under this Agreement. DHCS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties."

6. The terms used in this Agreement, but not otherwise defined, shall have the same meanings as those terms in HIPAA and/or the IPA. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

7. **Permitted Uses and Disclosures of PHI by Business Associate**. Except as otherwise indicated in this Agreement, Business Associate may use or disclose PHI, inclusive of de-identified data derived from such PHI, only to perform functions, activities or services specified in this Agreement on behalf of DHCS, provided that

such use or disclosure would not violate HIPAA or other applicable laws if done by DHCS.

7.1 Specific Use and Disclosure Provisions. Except as otherwise indicated in this Agreement, Business Associate may use and disclose PHI if necessary for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. Business Associate may disclose PHI for this purpose if the disclosure is required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person. The person notify the Business Associate of any instances of which the person is aware that the confidentiality of the information has been breached, unless such person is a treatment provider not acting as a business associate of Business Associate.

8. Compliance with Other Applicable Law

8.1 To the extent that other State and/or federal laws provide additional, stricter and/or more protective (collectively, more protective) privacy and/or security protections to PHI or other Confidential Information covered under this Agreement beyond those provided through HIPAA, Business Associate agrees:

8.1.1 To comply with the more protective of the privacy and security standards set forth in applicable State or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and

8.1.2 To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section 18. of this Agreement.

8.2 Examples of laws that provide additional and/or stricter privacy protections to certain types of PHI and/or confidential information, as defined in Section 4. of this Agreement, include, but are not limited to the Information Practices Act, California Civil Code sections 1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR part 2, W&I section 5328, and Health and Safety Code section 11845.5.

8.3 If Business Associate is a Qualified Service Organization (QSO) as defined in 42 CFR section 2.11, Business Associate agrees to be bound by and comply with subdivisions (2)(i) and (2)(ii) under the definition of QSO in 42 CFR section 2.11.

9. Additional Responsibilities of Business Associate

9.1 Nondisclosure. Business Associate not use or disclose PHI or other Confidential Information other than as permitted or required by this Agreement or as required by law.

9.2 Safeguards and Security.

9.2.1 Business Associate use safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and other confidential data and comply, where applicable, with subpart C of 45 CFR part 164 with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by this Agreement. Such safeguards be based on applicable Federal Information Processing Standards (FIPS) Publication 199 protection levels.

9.2.2 Business Associate, at a minimum, utilize a National Institute of Standards and Technology Special Publication (NIST SP) 800-53 compliant security framework when selecting and implementing its security controls and maintain continuous compliance with NIST SP 800-53 as it may be updated from time to time. The current version of NIST SP 800-53, Revision 5 is available online; updates will be available online at the NIST Computer Security Resource Centerhttps://csrc.nist.gov/publications/sp800.

9.2.3 Business Associate employ FIPS 140-2 validated encryption of PHI at rest and in motion unless Business Associate determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. FIPS 140-2 validation can be determined online at the NIST Cryptographic Module Validation Program page, with information about the Cryptographic Module Validation Program under FIPS 140-2 available online. In addition, Business Associate maintain, at a minimum, the most current industry standards for transmission and storage of PHI and other confidential information.

9.2.4 Business Associate apply security patches and upgrades, and keep virus software up-to-date, on all systems on which PHI and other Confidential Information may be used.

9.2.5 Business Associate ensure that all members of its workforce with access to PHI and/or other Confidential Information sign a confidentiality statement prior to access to such data. The statement be renewed annually.

9.2.6 Business Associate 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.

9.3 Business Associate's Agent. Business Associate ensure that any agents, subcontractors, subawardees, vendors or others (collectively, "agents") that use or disclose PHI and/or Confidential Information on behalf of Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such PHI and/or confidential information.

10. **Mitigation of Harmful Effects**. Business Associate mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI and other Confidential Information in violation of the requirements of this Agreement.

11. **Access to PHI.** Business Associate make PHI available in accordance with 45 CFR section 164.524.

12. **Amendment of PHI.** Business Associate make PHI available for amendment and incorporate any amendments to protected health information in accordance with 45 CFR section 164.526.

13. **Accounting for Disclosures.** Business Associate make available the information required to provide an accounting of disclosures in accordance with 45 CFR section 164.528.

14. **Compliance with DHCS Obligations.** To the extent Business Associate is to carry out an obligation of DHCS under 45 CFR part 164, subpart E, comply with the requirements of the subpart that apply to DHCS in the performance of such obligation.

15. **Access to Practices, Books and Records.** Business Associate make its internal practices, books, and records relating to the use and disclosure of PHI on behalf of DHCS available to DHCS upon reasonable request, and to the federal Secretary of Health and Human Services for purposes of determining DHCS' compliance with 45 CFR part 164, subpart E.

16. **Return or Destroy PHI on Termination; Survival.** At termination of this Agreement, if feasible, Business Associate return or destroy all PHI and other Confidential Information received from, or created or received by Business Associate on behalf of, DHCS that Business Associate still maintains in any form and retain no copies of such information. If return or destruction is not feasible, Business Associate notify DHCS of the conditions that make the return or destruction infeasible, and DHCS and Business Associate determine the terms and conditions under which Business Associate may retain the PHI. If such return or destruction is not feasible, Business Associate extend the protections of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

17. **Special Provision for SSA Data.** If Business Associate receives data from or on behalf of DHCS that was verified by or provided by the Social Security Administration (SSA data) and is subject to an agreement between DHCS and SSA, Business Associate provide, upon request by DHCS, a list of all employees and agents and employees who have access to such data, including employees and agents of its agents, to DHCS.

18. **Breaches and Security Incidents.** Business Associate implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and take the following steps:

18.1 Notice to DHCS.

18.1.1 Business Associate notify DHCS **immediately** upon the discovery of a suspected breach or security incident that involves SSA data. This notification will be provided by email upon discovery of the breach. If Business Associate is unable to provide notification by email, then Business Associate provide notice by telephone to DHCS.

18.1.2 Business Associate notify DHCS **within 24 hours by email** (or by telephone if Business Associate is unable to email DHCS) of the discovery of the following, unless attributable to a treatment provider that is not acting as a business associate of Business Associate:

18.1.2.1 Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person;

18.1.2.2 Any suspected security incident which risks unauthorized access to PHI and/or other confidential information;

18.1.2.3 Any intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement; or

18.1.2.4 Potential loss of Confidential Information affecting this Agreement.

18.1.3 Notice be provided to the DHCS Program Contract Manager (as applicable), the DHCS Privacy Office, and the DHCS Information Security Office (collectively, "DHCS Contacts") using the DHCS Contact Information at Section 18.6. below.

Notice be made using the current DHCS "Privacy Incident Reporting Form" ("PIR Form"; the initial notice of a security incident or breach that is submitted is referred to as an "Initial PIR Form") and include all information known at the time the incident is reported. The Privacy Incident Reporting Form is available online.

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI, Business Associate take:

18.1.3.1 Prompt action to mitigate any risks or damages involved with the security incident or breach; and

18.1.3.2 Any action pertaining to such unauthorized disclosure required by applicable federal and State law.

18.2 Investigation. Business Associate immediately investigate such security incident or breach.

18.3 Complete Report. To provide a complete report of the investigation to the DHCS contacts within ten (10) working days of the discovery of the security incident or breach. This "Final PIR" include any applicable additional information not included in the Initial Form. The Final PIR Form include an assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable federal and State laws. The report also include a full, detailed Corrective Action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that requested through the PIR form, Business Associate make reasonable efforts to provide DHCS with such information. A "Supplemental PIR" may be used to submit revised or additional information after the Final PIR is submitted. DHCS will review and approve or disapprove Business Associate's determination of whether a breach occurred, whether the security incident or breach is reportable to the appropriate entities, if individual notifications are required, and Business Associate's Corrective Action plan.

18.3.1 If Business Associate does not complete a Final PIR within the ten (10) working day timeframe, Business Associate request approval from DHCS within the ten (10) working day timeframe of a new submission timeframe for the Final PIR.

18.4 Notification of Individuals. If the cause of a breach is attributable to Business Associate or its agents, other than when attributable to a treatment provider that is not acting as a business associate of Business Associate, Business Associate notify individuals accordingly and pay all costs of such notifications, as well as all costs associated with the breach. The notifications comply with applicable federal and State law. DHCS approve the time, manner and content of any such notifications and their review and approval be obtained before the notifications are made.

18.5 Responsibility for Reporting of Breaches to Entities Other than DHCS. If the cause of a breach of PHI is attributable to Business Associate or its agents,

other than when attributable to a treatment provider that is not acting as a business associate of Business Associate, Business Associate is responsible for all required reporting of the breach as required by applicable federal and State law.

18.6 DHCS Contact Information. To direct communications to the above referenced DHCS staff, the Contractor initiate contact as indicated here. DHCS reserves the right to make changes to the contact information below by giving written notice to Business Associate. These changes shall not require an amendment to this Agreement.

DHCS Program Contract Manager	**DHCS Privacy Office**	**DHCS Information Security Office**
See the Scope of Work exhibit for Program Contract Manager information. If this Business Associate Agreement is not attached as an exhibit to a contract, contact the DHCS signatory to this Agreement.	Privacy Office c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (916) 445-4646	Information Security Office DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov

19. Responsibility of DHCS. DHCS agrees to not request the Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA and/or other applicable federal and/or State law.

20. Audits, Inspection and Enforcement

20.1 From time to time, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement. Business Associate promptly remedy any violation of this Agreement and certify the same to the DHCS Privacy Officer in writing. Whether or how DHCS exercises this provision shall not in any respect relieve Business Associate of its responsibility to comply with this Agreement.

20.2 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 promptly notify DHCS unless it is legally prohibited from doing so.

21. Termination

21.1 Termination for Cause. Upon DHCS' knowledge of a violation of this Agreement by Business Associate, DHCS may in its discretion:

21.1.1 Provide an opportunity for Business Associate to cure the violation and terminate this Agreement if Business Associate does not do so within the time specified by DHCS; or

21.1.2 Terminate this Agreement if Business Associate has violated a material term of this Agreement.

21.2 Judicial or Administrative Proceedings. DHCS may terminate this Agreement if Business Associate is found to have violated HIPAA, or stipulates or consents to any such conclusion, in any judicial or administrative proceeding.

22. Miscellaneous Provisions

22.1 Disclaimer. DHCS makes no warranty or representation that compliance by Business Associate with this Agreement will satisfy Business Associate's business needs or compliance obligations. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI and other confidential information.

22.2. Amendment.

22.2.1 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.

22.2.2 Failure by Business Associate to take necessary actions required by amendments to this Agreement under Section 22.2.1 shall constitute a material violation of this Agreement.

22.3 Assistance in Litigation or Administrative Proceedings. Business Associate make itself and its employees and agents 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 and/or employees based upon claimed violation of HIPAA, which involve inactions or actions by the Business Associate.

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

22.5 **Interpretation**. The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and other applicable laws.

22.6 **No Waiver of Obligations**. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.