IEHP SUBCONTRACTOR MANUAL POLICY
HIPAA Program Requirements

Introduction

This Health Insurance Portability and Accountability Act (HIPAA) Program sets forth the requirements in which IEHP expects Subcontracted entities to develop and maintain their Programs.

Inland Empire Health Plan (IEHP) has adopted and maintains policies and procedures required by the Health Insurance Portability and Accountability Act (HIPAA) and the American Recovery and Reinvestment Act (ARRA) to:

A. Ensure that Member's health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care;

B. Comply with the requirements of ARRA including, but not limited to, Member requests for restrictions and accounting of disclosures;

C. Protect the public's health and wellbeing;

D. Adhere to the HIPAA General Administrative Requirements as published in the final rule on December 28, 2000 and amended on May 31, 2002 and August 14, 2002 and January 25, 2013. These requirements are found in Title 45 of the Code of Federal Regulations (C.F.R.) Part 160, Part 162, and Part 164.

E. Comply with the administrative, physical and technical safeguards of the HIPAA Security Rule, as required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act);

F. Comply with the Department of Health Care Services (DHCS); Centers for Medicare & Medicaid Services (CMS); and, the HITECH Act breach reporting requirements; and,

G. Provide HIPAA training to IEHP Team Members, Governing Board Members, business associates, first tier and downstream entities and vendors with access to Member PHI.

HIPAA Program

A. **Purpose**

1. To accept and comply with a common set of general provisions and definitions related to HIPAA and ARRA guidelines.
2. To identify and apply:
   a) Any HIPAA preemption requirements to State law; and
   b) Any State law that is more stringent than the requirements of HIPAA.
3. To establish IEHP Compliance and Enforcement procedures based upon HIPAA and ARRA Standards and Implementation Specifications.

B. **Scope**

1. The HIPAA Program, which falls under the auspices of the Compliance Department's Special Investigations Unit (SIU), applies to:

a) All IEHP Members;

b) Every health care provider, regardless of size, who holds or transmits Member protected health information (PHI) in any form of media, whether electronic, paper or oral (covered entities); and,

c) IEHP business associates, Subcontractor, Downstream entities, and vendors that perform certain functions or activities on behalf of IEHP that involve the use or disclosure of Member identifiable health information.

C. **Organizational Structure and Resources**

1. The day-to-day oversight of the HIPAA Program is the direct responsibility of the HIPAA Privacy Officer, who reports compliance issues and activities to the Compliance Officer, the Chief Executive Officer (CEO), Compliance Committee, and Governing Board. The HIPAA Privacy Officer oversees all aspects of the HIPAA Program including but not limited to:

   a) Uses and disclosures of protected health information (PHI);

   b) Privacy policies and procedures, including but not limited to complaint procedures and compliance with Federal and State reporting requirements;

   c) Team Member, business associate, first tier and downstream entity, training program;

   d) Mitigation of any harmful effects caused by use or disclosure of PHI by IEHP Team Members or external associates in violation of IEHP privacy policies and procedures; and,

   e) Maintenance of reasonable and appropriate administrative, technical and physical safeguards to prevent intentional or unintentional use or disclosure of PHI.

2. The HIPAA Privacy Officer has ultimate responsibility for the HIPAA Program.

3. The IEHP Governing Board and CEO will provide oversight of the HIPAA Program.

D. **Definitions**

1. Access and Uses: For internal uses, IEHP allows Team Member access to PHI subject to qualifying job requirements. Each Team Member is provided appropriate levels of access to perform their job duties.

2. Authorization: IEHP must obtain the Member's written authorization for any use or disclosure of PHI that is not for treatment, payment, health care operations or otherwise permitted or required by regulations and/or statutes. Authorizations must be written in specific terms; must be in plain language; and must contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data in accordance with the requirements of HIPAA (45 C.F.R. § 164.508) and California Confidentiality of Medical Information Act (Civil Code § 56.11).

   In most cases, parents can exercise individual rights, such as access to the medical record on behalf of their minor children. However, there are circumstances under which the parent is not considered the personal representative. In these situations, IEHP will defer to California State law to determine the rights of parents to access and control the PHI of their minor children.

3. Breach: The term "breach" has the meaning given such term in 45 C.F.R. § 164.402.

a. "Breach" means the acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted under 45 C.F.R. Part 164, Subpart E ("Privacy Rule") which compromises the security or privacy of the PHI. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity can demonstrate that there is a low probability that the protected health information has been compromised (45 C.F.R. § 164.402.; 78 Fed Reg. at 5641). Covered entities must consider a four- factor objective standard (78 Fed. Reg. at 5642):

1. the nature and extent of protected health information involved (including the types of identifiers and the likelihood of re-identification);
2. the unauthorized person who used the protected health information or to whom the disclosure was made;
3. whether the protected health information was actually acquired or viewed; and,
4. the extent to which the risk of breach to the protected health information has been mitigated.

b. Exception: Breach excludes (45 C.F.R. § 164.402):

1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of protected health information where the covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

c. If the acquisition, access, use or disclosure of protected health information is excluded from the definition of "breach" under paragraph 3.b. above, the reporting requirements of DHCS, and / or CMS do not apply.

4. Business Associate: The term "business associate" has the meaning given such term in 45 C.F.R. § 160.103.

a. Except as provided in paragraph 4(b) of this definition, business associate means, with respect to a covered entity, a person who:

1. On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits, protected health information for a function or activity regulated by Title 45, Subtitle A, Subchapter C (HIPAA Administration Data Standards and Related

Requirements), including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and re-pricing; or

2. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR 164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the services involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person; or
3. Provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information (including a Health Information Organization or E-prescribing Gateway); or
4. Offers a personal health record to one or more individuals on behalf of a covered entity; or
5. Is a subcontractor that creates, receives, maintains, or transmits, protected health information on behalf of the business associate; or
6. A covered entity may be a business associate of another covered entity.

b. Business associate does not include:

1. Health care providers, with respect to disclosures by a covered entity to the health care provider, concerning the treatment of the individual.
2. Plan sponsors, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, under certain circumstances.
3. Government agencies, with respect to determining eligibility for, or enrollment in a government health plan providing public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are unauthorized by law.
4. A covered entity participating in an organized health care arrangement that performs a function or activity as described in paragraph (a)(1), above, for or on behalf of such organized health care arrangement, or that provides a service as described in (a)(2), to or for such organized health care arrangement by virtue of such activities or services.

5. Confidentiality: Relates to the obligation of the holder of personal information to protect an individual's privacy. This obligation is determined by common practice, and Federal and State laws and regulation.
6. Covered Entity: The term "covered entity" has the meaning given such term in 45 C.F.R § 160.103.

a. A health Plan

b. A health care clearinghouse.

c. A healthcare provider who transmits any health information in electronic form in connection with a transaction covered by Title 45, subtitle A. Subchapter C (HIPAA Administrative Data Standards and Related Requirements).

7. Disclosure: The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information (45 C.F.R. § 160.103).
8. Downstream Entity is any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the MA benefit or Part D benefit, below the level of the arrangement between an MAO or applicant or a Part D plan sponsor or applicant and a first-tierentity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services. (42 C.F.R. §, 423.501).
9. Electronic Health Record (EHR): An electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff (42 U.S.C. § 17921(5)).
10. Subcontractor
    a. CMS Definition: is any party that enters into a written arrangement, acceptable to CMS, with an MAO or Part D Plan sponsor or applicant to provide administrative services or health care services to a Medicare eligible individual under the MA program or Part D program. (42 C.F.R§,423.501).
    b. DHCS Definition: an individual or entity that has a Subcontractor Agreement with Contractor that relates directly or indirectly to the performance of Contractor's obligations under this Contract. A Network Provider is not a Subcontractor solely because it enters into a Network Provider Agreement.
11. Health Care Operations: Includes activities of the covered entity to the extent that the activities are related to covered functions:
    a. Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; Patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.
    b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner/provider performance, health plan performance, conducting training programs under supervision to practice or improve health care provider skills, training of non-health care professionals, accreditation, certification, licensing or credentialing activities.
    c. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs.
    d. Business planning and development including formulary development and administration, development or improvement of methods of payment or coverage policies.
    e. Business management and general administrative activities of the entity as outlined in 45

C.F.R. §164.501.

12. Health Care Provider: A provider of medical or health services; pursuant to Title 42 United States Code (U.S.C.) Section 1395x subsections (s) and (u); and, any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. (45 C.F.R. §160.103).
13. Health Plan: An individual or group plan that provides, or pays the cost of, medical care as defined in Title 42 U.S.C. §300gg-91(a)(2) (45 C.F.R. §160.103).
14. Individual: The person who is the subject of the protected health information (45 C.F.R. § 160.103).
15. Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and:
    a. Is created or received by a health care provider, health plan, employer or health care clearinghouse; and
    b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    c. That identifies the individual; or,
    d. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
16. Payment: Has the meaning given such term in 45 C.F.R. §164.501.
17. Personal Health Record (PHR): An electronic record of PHR identifiable health information (as defined in section 42 U.S.C. § 17921(11)) on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.
18. Personal Representative: A person legally authorized to make health care decisions on a Member's behalf or to act for a deceased Member or the estate. The Privacy Rule permits an exception should IEHP have a reasonable belief that the personal representative may be abusing or neglecting the Member, or that treating the person as the personal representative could otherwise endanger the Member.
19. PHR Identifiable Health Information: Individually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes, with respect to an individual, information that is provided by or on behalf of the individual; and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
20. Privacy: Relates to an individual's desire to control access to their personal information.
21. Protected Health Information (PHI): All individually identifiable health information, (including genetic information) whether oral or recorded in any form, that relates to the physical or mental health of a Member, the provision of health care to that Member, or the payment for the provision of health care services to an individual (45 C.F.R. § 160.103).
    a. PHI excludes individually identifiable health information in education records covered by

the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and, employment records held by a Covered Entity in its role as employer.

b. Security: Security or security measures, encompasses all of the administrative, physical and technical safeguards in an information system (45 C.F.R. § 164.304). It relates to the extent to which information can be stored and provided with access limited to those who are authorized and have a legitimate need to use/disclose such information.

E. **Procedure**

1. IEHP will use HIPAA definitions, as found in 45 C.F.R. §160.103, 164.402 and 164.501.
   a) Any modifications from the Department of Health and Human Services (DHHS) to the existing definitions will be incorporated into new IEHP policy creation; any applicable existing IEHP policy will be edited/revised accordingly.
   b) IEHP will use the HIPAA definitions in general use and as reference to determining if HIPAA preempts State Law.
2. Uses and Disclosure
   a) Basic Principle for Use and Disclosure: IEHP may not use or disclose PHI, except either: (1) as the Privacy Rule permits or requires; or (2) as the Member who is the subject of the information (or the Member's personal representative) authorizes in writing.
   b) Required Disclosures: IEHP must disclose PHI in only two (2) situations: (a) to Members (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and, (b) to a contracted government agency when it is undertaking a healthcare compliance investigation or review or enforcement action.
   c) Permitted Uses and Disclosures: IEHP is permitted, but not required, to use and disclose PHI, without a Member's authorization, for the following purposes or situations: (1) To the Member, with limited exceptions; (2) Treatment, Payment and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Limited Data Set for the purposes of research, public health or health care operations. IEHP may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make. (In accordance with PRO_CMP P-02- "Uses and Disclosure of Protected Health Information (PHI)(NCQA)".
3. Minimum Necessary: IEHP will make all reasonable efforts to use, disclose and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure or request. The minimum necessary requirement does not apply in any of the following circumstances:
   a) Disclosure to or a request by a health care provider for treatment;
   b) Disclosure to a Member who is the subject of the information, or the Member's personal representative;
   c) Use or disclosure made pursuant to an authorization;
   d) Disclosure to a contracted government agency for healthcare related complaint investigation, compliance review or enforcement;

e) Use or disclosure that is required by law; or,

f) Use or disclosure required for compliance with the applicable requirements of HIPAA Administrative Data Standards and Related Requirements (45 C.F.R. Subtitle A, Subchapter C).

4. Accounting of Disclosures of PHI: Upon Member request, it is the policy of IEHP to provide Members with an accounting of PHI disclosures made by IEHP within the last six (6) years (or shorter period of time if a shorter period is requested) prior to the date on which the accounting is requested. See policies PRO_CMP P-02 "Uses and Disclosure of Protected Health Information (PHI) (NCQA)" and PRO_CMP P-06 "Accounting of Disclosures of PHI".

5. Privacy Practices Notice: IEHP provides the "Notice of Privacy Practice" to each new Member as follows:

   a) At enrollment and annually thereafter;

   b) Within 60 days of a material change to the uses or disclosures, the Member's rights, IEHP's legal duties, or other material privacy practices stated in the Notice; and,

   c) Upon request by any person including IEHP Members.

   The IEHP Member Handbook details the plan's security and privacy practices and refers Members to Member Services and/or the IEHP Internet website for further information. See policy PRO_CMP P-04 "Notice of Privacy Practices (NCQA)"**.**

6. Access. It is the policy of IEHP to allow Members or their legal representative to inspect and receive a copy of their PHI within the IEHP *designated record set* upon request, with some exceptions. Members, or their legal representatives, will be requested to submit their request in writing and to submit proof of identity for the release. The "designated record set" is a group of records maintained by IEHP that are used to make decisions about Member enrollment; provider payments; claims adjudication; and, case or medical management systems.

7. The Privacy Rule excepts from the right of access the following PHI (45 C.F.R. §164.524):

   a) Psychotherapy notes maintained separate from other mental health records;

   b) Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative actions or proceedings;

   c) Laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access; or,

   d) Information held by certain research laboratories.

8. IEHP may deny access to a Member or their legal representative in certain specified situations, such as when a health care professional believes that access could cause harm to the Member or another. In such cases, the Member or their legal representative are given the right to have such denials reviewed by a licensed health care professional. IEHP will provide or deny access based on the reviewing official's determination. (In accordance with PRO_CMP P-03 "Securing PHI" and LegalDRS_02 "IEHP Designated Record Set").

9. Covered entities are permitted to disclose a decedent's information to family members and others involved in the decedent's care prior to death unless the decedent previously expressed

otherwise (45 C.F.R § 164.510(b)(5)).

F. **Amendment**

1. IEHP Members have a right to amend their PHI in a designated record set when that information is inaccurate or incomplete (45 C.F.R. § 164.526). If an amendment is granted in whole or in part, IEHP must:
   a) Amend the information or the record that is the subject of the request;
   b) Notify the Member that the amendment has been accepted; and,
   c) Notify relevant persons, Providers, business associates or organizations identified by either the Member or IEHP, of the amendment.
2. IEHP may deny an amendment based on the following instances:
   a) Information requested to be amended was not created by the Provider;
   b) Information requested to be amended is not part of the designated record set;
   c) Information requested to be amended is not information that the Member has a right to access; or,
   d) Information requested to be amended is accurate and complete.
3. If the request is denied, IEHP will provide the Member with the basis for the denial and inform the Member of their right to submit a statement of disagreement which shall be filed, and subsequently released with, the record; and, a description of how the Member can commence a complaint to IEHP or to the Secretary of DHHS.
4. IEHP will amend PHI in its designated record set upon receipt of notice to amend from another covered entity. (In accordance with PRO_CMP P-05 "Member's Request to Amend, Restrict Access or Deny Access to PHI").

G. **Restriction Request**

In the case that a Member requests under 45 C.F.R. § 164.522 (a)(1)(i)(A), that IEHP restrict the disclosure of his/her PHI, notwithstanding paragraph (a)(1)(ii) of such section, IEHP must comply with the requested restriction if:

1. Except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and,
2. PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.
3. Members have the right to request that IEHP restrict use or disclosure of PHI to notify family members or others about the Member's general condition, location or death.
4. IEHP will not agree to the restriction or denial of PHI as requested by the Member if IEHP determines that the information being restricted would impede treatment for the Member being served. See policy PRO_CMP P-05 "Member's Requests to Amend, Restrict Access or Deny Access to PHI".

H. **Confidential Communications**

1. IEHP permits Members to request an alternative means or location for receiving communications of PHI by means other than those that IEHP typically employs.
2. IEHP will accommodate reasonable requests if the Member indicates that the disclosure of all or part of the PHI could endanger the Member. IEHP will not question the Member's statement of endangerment. See policy PRO_CMP P-05 "Member's Requests to Amend, Restrict Access or Deny Access to PHI".

I. **Administrative Requirements**

1. Privacy Policies and Procedures: IEHP has developed and implemented policies and procedures that are consistent with The Privacy Rule.
2. Privacy Personnel: IEHP has designated the HIPAA Privacy Officer as their privacy official responsible for developing and implementing its privacy policies and procedures.
3. IEHP has designated its Compliance Department as the office responsible for receiving HIPAA related complaints and providing Members and other individuals with information on IEHP HIPAA practices. See policy PRO_CMP C-07 "Duties of Compliance Officer – HIPAA (NCQA)".
4. Team Member Training: Training requires that all IEHP Team Members, including management, demonstrate awareness and understanding of HIPAA Privacy and Security standards, as well as privacy requirements under the HITECH Act and ARRA. Additionally, business associates, first tier and downstream entities and vendors who have access to Member PHI must document that their workforce members have been trained on these standards.
    a) During "New Hire Orientation," every newly hired Team Member is provided with reference documents regarding HIPAA and PHI.
    b) Newly hired IEHP Team Members are required to sign a "Protected Health Information (PHI) Confidentiality Statement," at the time of their IEHP orientation process and annually thereafter. Team Members are also required to sign an acknowledgment form acknowledging receipt and recognition of the IEHP Code of Conduct.
    c) Upon hire, and annually thereafter, each Team Member is required to complete compliance training.
    d) IEHP informs Team Members, through the Team Member Handbook, that unauthorized disclosure of PHI or other confidential information is grounds for immediate disciplinary action, up to and including termination."
    e) IEHP Team Members are provided with notification when material changes have been made to the privacy procedures within a reasonable period of time following approval by the HIPAA Privacy Officer and the Compliance Committee.
    f) The availability of reporting privacy and/or security concerns regarding HIPAA non-compliance is included in all training sessions, as well as, appearing on the internal website. IEHP has a zero-tolerance policy for retaliatory action against Team Members who report HIPAA concerns.
    g) Other training materials for Team Members include, but are not limited to, periodic security updates and reminders.

5. Business Associate, First Tier and Downstream Entities and Vendor Training: IEHP provides HIPAA learning experiences including, but not limited to:
    a) Pre-contractual and annual audits of IPA HIPAA compliance, to include corrective action plans (CAPs) for identified deficiencies.
6. Provider Training: Privacy incidents/breaches of Member information by a Provider may result in a CAP.
7. Mitigation: IEHP shall mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of PHI by its Team Members or its business associates and subcontractors in violation of its privacy policies and procedures or the Privacy Rule.
8. Data Safeguards: IEHP maintains administrative, technical and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit incidental use and disclosure. Policies and procedures have been developed and implemented.
    a) IEHP utilizes a document cross shredding service and uses securely locked shredder bins in each business area to hold confidential documents prior to shredding.
    b) Hard copy documents containing PHI are secured under lock and key during non-business hours; and all Team Members have been provided with "PHI Protectors" to be placed over any and all confidential documents that are in process at their desks.
    c) The IEHP Information Technology Department has implemented technical safeguards to protect PHI and has policies and procedures in place for electronic security from unauthorized disclosure, i.e., passwords; screen time-outs; secure E-Mail; etc. Team Member responsibilities for electronic security are included in compliance training for Team Members and are detailed in IT policies and procedures.
    d) IEHP protects the privacy of individual Member PHI by de-identifying PHI when released for purposes other than treatment, payment or healthcare operations; for use without the Member's authorization; and, for purposes other than those legally required under HIPAA to protect public safety.
    e) The IEHP Team Member Handbook addresses the policy for verbal disclosures of PHI, including Team Member discussion outside the IEHP offices.
    f) IEHP has implemented a policy that addresses verifying the identity of the individual requesting PHI prior to release of the information. By administering this policy, Team Members put forth their best efforts to send PHI, in any format, to the appropriate requestor.
    g) The Facilities Department has implemented physical safeguards for PHI including, but not limited to, controlled access to all areas of the buildings as detailed in their Policies and Procedures.
9. Compliance:
    a) The Compliance Department conducts monthly in-house, random departmental HIPAA walk-throughs to assess Team Member compliance with the IEHP PHI privacy policy. See policy PRO_CMP P-08 "Monitoring and Auditing for Health Insurance Portability and Accountability Act (HIPAA) Privacy Compliance: HIPAA Walk-Throughs".
    b) IEHP requires that business associates who may be recipients of PHI must agree, in writing,

to certain mandatory contract provisions regarding the use and disclosure of PHI.

c) IEHP monitors contracted IPAs and business associates for compliance with HIPAA regulations prior to contracting and annually thereafter.

10. Notification of Privacy Breach: IEHP maintains and implements policies and procedures for providing notification of suspected and/or actual privacy breaches for all lines of business to the appropriate regulatory agencies. The IEHP Compliance Department investigates such breaches or unauthorized uses or disclosures of PHI and, when necessary, requires that a Root Cause Analysis and a Corrective Action Plan be completed and submitted by the department responsible for the breach. See policy PRO_CMP P-09 Privacy Incidents - Risk Assessment and Breach Reporting.
11. Notification to the Media & California State Attorney: IEHP maintains and implements policies and procedures for providing notification of a breach of protected health information of more than 500 individuals within the State of California or jurisdiction to the media serving the area, without unreasonable delay, but no later than 60 days after discovery. (74 Fed. Reg. at 42768). In addition, notification to the California State Attorney will be made.
12. HIPAA Non-Compliance: IEHP has a policy and procedure in place for Members, Team Members, Business Associates or other individuals to submit concerns and/or incidents of non-compliance with HIPAA requirements to the plan and/or to the Secretary of DHHS. See policy PRO_CMP P-04a "Notice of Privacy Practices". Issues involving HIPAA and/or non-compliance may be reported by the following methods:

    Compliance Hotline: 866-355-9038

    Fax: 909-477-8536

    Compliance Mailbox: compliance@iehp.org

    In Person: Special Investigations Unit Compliance Team

    Mail: IEHP HIPAA Privacy Officer, PO Box 1800, Rancho Cucamonga, CA 91729-1800

    JIVE: Click on the Compliance Corner link.

    Webform: IEHP.org Provider Resources – Compliance.

13. Retaliation and Waiver: IEHP does not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by DHHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. IEHP does not require a Member to waive any right under the Privacy Rule as a condition for obtaining treatment, payment and enrollment or benefits eligibility.
14. Documentation and Record Retention: IEHP maintains archives of privacy policies and procedures, privacy practice notices, disposition of complaints and other actions, activities, and designations that the Privacy Rule requires for a period of ten (10) years.
15. Destruction of Confidential Information: Each area creating, receiving, and retaining

confidential information of any type including PHI is responsible to protect the information and deposit the information in secured shredding bins.

INLAND EMPIRE HEALTH PLAN		
Written By: Director, Compliance & Risk Management	**Original Effective Date:**	January 1, 2022
Approved By: Vice President Compliance/Compliance Officer	**Approval Date:**	
	Revision Date:	N/A