23. COMPLIANCE

A. Monitoring of First Tier, Downstream and Related Entities

APPLIES TO:

A. This policy applies to all IEHP DualChoice Cal MediConnect Plan (Medicare–Medicaid Plan) Providers; and First Tier, Downstream, and Related Entities (FDRs).

POLICY:

A. IEHP may delegate the authority and responsibility to carry out program/plan activities that are otherwise performed by IEHP. IEHP retains accountability for services provided by First Tier, Downstream and Related Entities (FDRs). Further, IEHP is responsible for maintaining compliance with applicable State and Federal requirements.

1. The terms and conditions set forth in contracts with FDRs require that they perform and maintain delegated functions consistent with IEHP’s contractual obligations.

B. IEHP will conduct a pre-contractual evaluation and annual audit of all IPAs and FDRs, as appropriate. IEHP monitors FDR performance on an ongoing basis and will implement corrective actions and revoke delegation of duties if it determines that an FDR is unable or unwilling to carry out its responsibilities.

C. An annual risk assessment will be completed to aid in identifying high risk FDRs. High risk FDRs are those that possess characteristics such as; responsibility for tasks that aid in or have a potential for hindering member access to service, are continually non-compliant or at risk of non-compliance based on regulatory and IEHP requirements, or have a history of non-compliance as identified by a government agency. FDRs determined to be high risk may be subjected to a more frequent monitoring and auditing schedule. This risk assessment process will be managed by the Delegation Oversight Committee and presented to the Compliance Committee for review and discussion.

D. The Compliance Department works in conjunction with the Delegation Oversight Committee to evaluate, recommend and implement improvements to the process for monitoring delegated FDRs. In addition, the Compliance Department along with the Delegation Oversight Committee develop the annual audit calendar, which includes FDR monitoring activities to validate compliance with contractual standards and regulatory requirements.

E. The Delegation Oversight Committee is tasked with oversight of the FDR Oversight process. The Committee reviews data as reported by the FDR Committee and recommends modifications where appropriate. The key functions of the Delegation Oversight Committee for oversight of delegation management include:

1. Monthly reviews of FDR performance data.

2. Review and approval of corrective actions; review recommendations for contractual penalties; assistance with the implementation of corrective actions and penalties; etc.

3. Approval of the annual audit calendar and any ad-hoc FDR monitoring and auditing.
23. COMPLIANCE

A. Monitoring of First Tier, Downstream and Related Entities

4. Determining approval for delegated and sub-delegated activities for new FDRs based on the initial evaluation, assessment and approval of the operational functional leads.

5. Results and actions taken by the Delegation Oversight Committee are reported up to the Compliance Committee.

6. Provide reports at least annually to the IEHP Governing Board regarding monitoring and auditing activities conducted as part of the FDR Oversight program.

F. The Compliance Department enforces the compliance program by ensuring all regulatory requirements and policies and procedures are adhered to. There are a variety of ways in which this is achieved, including:

1. Annually reviews and updates the Program, as applicable.

2. Annually reviews and updates associated policies and procedures, as applicable, incorporating ad-hoc changes as regulatory changes require.

3. Presents program efforts to the Compliance Committee.


G. The functional areas and business departments implement the FDR Oversight program at an operational level. Oversight activities outlined in the plan are managed by the responsible business areas. The departments are responsible for the following:

1. Managing the day-to-day FDR relationship.

2. Identifying negative trends or vulnerabilities.

3. Monitoring FDR compliance according to the Program and associated tools and processes.


5. Day-to-day management of issues and actions; escalated as required.

6. Assisting with implementation, review and acceptance of corrective action plans.

7. Managing FDR operational communications and/or training.


9. Assisting the Compliance Department in identifying risk as part of the annual risk assessment.

PURPOSE:

A. The purpose of this policy is to ensure that FDRs are compliant with meeting the terms and conditions of regulatory elements as established by CMS, the State of California, other governmental entities, and IEHP.
23. COMPLIANCE

A. Monitoring of First Tier, Downstream and Related Entities

PROCEDURES:

A. Initial Evaluation: Prior to executing a contract or delegation agreement with a potential FDR, requests for an initial evaluation may be forwarded to the Delegation Oversight Committee by the department executing the contract or delegation agreement. The Delegation Oversight Committee may ensure an initial evaluation as necessary to determine the ability of the potential FDR to assume responsibility for delegated activities and to maintain IEHP standards, applicable State, CMS and accreditation requirements.

1. The following will be assessed in the initial evaluation:
   a. The entity’s ability to perform the required tasks. IEHP will verify that the FDR meets both contractual and regulatory requirements.
   b. Policies and procedures specific to the delegated function(s).
   c. Operational capacity to perform the delegated function(s).
   d. Resources (administrative and financial) sufficient and qualified to perform the required function(s).
   e. Exclusion of the FDR from participating in State and/or Federal health programs (excluded parties lists):
      1) The Department of Health and Human Services (DHHS) Office of Inspector General (OIG) List of Excluded Individuals and Entities (LEIE);
      2) The General Services Administration (GSA) Excluded Parties List System (EPLS);
      3) The Medicare Opt-Out List; and
      4) The DHCS Medi-Cal Suspended and Ineligible Provider List.
   f. The entity’s annual compliance and FWA training program.

2. An initial onsite evaluation may be conducted. If the FDR is not in full compliance with delegated standards, the FDR's action plan and timeline to achieve full compliance is reviewed. The oversight process may be modified for accredited/certified FDRs as applicable. The need for an onsite visit and/or file audit is at the sole discretion of IEHP. IEHP determines the frequency and format of contact with the FDR to verify compliance with established, revised, or new State, CMS, and accreditation requirements. The FDR is required to comply with IEHP reporting requirements.

3. Results of the initial evaluation are documented in an audit report and presented to the Delegation Oversight Committee and subsequently the Compliance Committee for review and/or approval. To accommodate business needs, ad hoc meetings or electronic review and/or approval may substitute for routinely scheduled meetings.
23. COMPLIANCE

A. Monitoring of First Tier, Downstream and Related Entities

B. Contract: The contract specifies the delegated activities, responsibilities of the parties, reporting frequency, the process for evaluation, and remedies available to IEHP for inadequate delegate performance, up to and including revocation of delegation or imposition of other sanctions. First Tier entities may not delegate their contractually assigned functions to another organization without the approval of IEHP. A monitoring schedule and process of the downstream or related entity's compliance requirements will be determined by IEHP.

C. Data: Once delegation is approved and a contract is executed, the FDR must submit data as contractually required.

D. Risk Areas: In identified risk areas, additional reporting may be required from the FDR. The FDR may be obligated to submit a report summarizing activities completed during the quarter, identifying barriers to improvement and the effectiveness of any improvement plans. These reports will be reported to the Delegation Oversight Committee.

E. Audit Calendar: IEHP conducts a comprehensive review of the FDR's ability to provide delegated services in accordance with contractual standards and applicable State, CMS, and accreditation requirements. High risk FDRs, as determined by the annual risk assessment and/or continued non-compliance, will obtain priority status on the annual audit calendar. In conjunction with policies and procedures, IEHP will not limit its audit calendar to high risk FDRs.

F. Annual Audits: The following will be assessed during an annual audit:
   1. The entities' ability to perform the required tasks. IEHP will verify the FDR meets both contractual and regulatory requirements.
   2. Policies and procedures specific to the delegation function(s).
   3. Operational capacity to perform the delegated function(s).
   4. Resources (administrative and financial) sufficient and qualified to perform the required function(s).
   5. Annual Ownership and Control documentation.
   6. Exclusion of the FDR from participating in the federal health program (excluded parties lists):
      a. The DHHS OIG LEIE;
      b. The GSA EPLS;
      c. The Medicare Opt-Out List; and
      d. The DHCS Medi-Cal Suspended and Ineligible Provider List.
   7. Effective training and education that includes:
      a. General compliance.
23. COMPLIANCE

A. Monitoring of First Tier, Downstream and Related Entities

b. Fraud, Waste and Abuse.

c. Training Material.
   1) Presentations.
   2) Sign-In Sheets.
   3) Presenter Certifications.

G. Focused Audits: If IEHP has a reason to believe the FDR's ability to perform a delegated function is compromised, a focused audit may be performed. The results of these audits will be reported to the Delegation Oversight Committee. The Compliance Department may also recommend focused audits upon evaluation of non-compliant trends or reported incidents.

1. Focused audit criteria include, but are not limited to, the following:
   a. Failure to comply with regulatory requirements and/or the IEHP service level performance indicators.
   b. Failure to comply with a corrective action plan.
   c. Reported or alleged fraud, waste and/or abuse.
   d. Significant policy variations that deviate from the IEHP, State, CMS or accreditation requirements.
   e. Bankruptcy or impending bankruptcy which may impact services to Members (either suspected or reported).
   f. Sale, merger or acquisition involving the FDR.
   g. Significant changes in the management of the FDR.
   h. Changes in resources which impact operations.

H. Attestation Audits: Attestation audits are a form of validation audit that is performed to validate the information/data in the submitted attestation form are accurate and complete, therefore the scope, the sample size and the documents required at the time of the audit may vary depending on the nature of the attestation. The attestations must be signed by an authorized representative and certifies information such as training and policies and procedures are in compliance.

I. Annual Risk Assessment: The Delegation Oversight Committee will manage the annual comprehensive risk assessment process to determine the FDR's vulnerabilities and high risk areas. A look-back period is determined which includes any corrective actions; service level performance; reported detected offenses; complaints and appeals, from the previous year. Any FDR deemed high risk or vulnerable is presented to the Compliance Committee for suggested action.
23. **COMPLIANCE**

A. Monitoring of First Tier, Downstream and Related Entities

J. Corrective Action: A corrective action plan is developed by the delegated entity and reviewed and approved by the Delegation Oversight Committee in instances where non-compliance is identified. Each corrective action plan is presented to the Delegation Oversight Committee for approval. Supplementary, focused audits and additional reporting and/or targeted auditing may be required until compliance is achieved.

1. At any time IEHP may require remediation by an FDR for failure to fulfill contractual obligations including development and implementation of a corrective action plan. Failure to cooperate with IEHP in any manner may result in further remedial action leading up to and including termination of the agreement and/or return of delegated activities to IEHP.

K. Training: IEHP will make training materials available to FDRs. However, it is expected that FDRs institute their own training program intended to communicate the compliance characteristics related to the FDR and their contractually delegated area(s). Training materials will be reviewed by IEHP during the audit process.

1. IEHP will distribute an annual attestation to the FDRs. The completed, returned attestation confirms compliance with new hire and annual training and education requirements to include General Compliance; Fraud, Waste and Abuse; and, HIPAA.

2. FDR training documentation will be requested and evaluated as part of the annual audit process. Material for review may include, but not be limited to, training presentations; sign-in sheets; test scores; trainer proficiencies; new hire orientation packets; employee list (including date of hire and date of previous training).

3. First Tier Entities are required to implement a training program that ensures its subcontracted downstream and related entities are also trained and have instituted a similar training program.

**REFERENCES:**

B. IEHP Coordinated Care Initiative (CCI) Three-Way Contract.
C. Medicare Managed Care Manual Chapter 21.
F. California Code of Regulations, Title 10, et al.
G. California Code of Regulations, Title 22, §§ 51000-53999.
23. COMPLIANCE

A. Monitoring of First Tier, Downstream and Related Entities

I. Welfare and Institutions Code, § 14100 et seq., 14458.
23. COMPLIANCE

B. HIPAA Privacy and Security

APPLIES TO:

A. This policy applies to IEHP DualChoice Cal MediConnect Plan (Medicare – Medicaid Plan) Members and Providers, Business Associates, First Tier Entities, Downstream Entities, Contractors and Health Care Entities, hereby referenced as “entities”.

POLICY:

A. This policy is based on the following principles and procedures related to the access, use and disclosure of Member information.

1. To provide guidance regarding each entity’s responsibility related to identifiable Member information, this policy addresses intentional and unintentional breaches of Member confidentiality, including oral, written and electronic communication. The principles in this policy will help safeguard Member privacy and minimize exposure and/or liability to Members, entities and IEHP.

2. Entities must make reasonable efforts to safeguard the privacy and security of Members’ PHI and are responsible for adhering to this policy by using only the minimum information necessary to perform their responsibilities, regardless of the extent of access provided or available.

3. Entities must comply with the Health Insurance Portability and Accountability Act (“HIPAA”) laws and regulations including, but not limited to the privacy and security of Members’ PHI as required by HIPAA, Standards for Privacy of Members’ Identifiable Health Information, 45 CFR Parts 160, 162 and 164; 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) as part of the American Recovery and Reinvestment Act of 2009; and any and all Federal regulations and interpretive guidelines promulgated there under.

4. Entities are allowed to release Member PHI to IEHP, without prior authorization from the Member, if the information is for treatment, payment or health care operations related to IEHP plans or programs.

5. Entities must notify IEHP, their Members, the Centers for Medicare and Medicaid (CMS), and the U.S. Department of Health & Human Services (DHHS) of any suspected or actual breach regarding the privacy and security of a Member’s PHI within prescribed timelines and through acceptable submission formats.

B. Due to unauthorized disclosures of protected patient medical records, confidentiality requirements were enhanced by California Health and Safety Code, Section 1280.15. The bills make Providers accountable for unauthorized access to medical information, not just for unlawful use or disclosure.

1. Every healthcare entity must implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient’s medical record information and
23. COMPLIANCE

B. HIPAA Privacy and Security

safeguard it from unauthorized access or unlawful access, use, or disclosure. Administrative fines for violations vary significantly.

2. IEHP may impose sanctions, up to and including corrective action or termination, against entities for failure to comply with applicable privacy and security laws and regulations. The extent and scope of sanctions depend on the type of violation and the conduct of the entity.

3. All healthcare entities should educate their employees on privacy laws and their policy on privacy of medical information. The education should be documented and should include attendance.

4. Appropriate, documented action must be taken should unauthorized access occur.

DEFINITION:

A. Business Associate: A person or entity that performs certain functions or activities that involve the use or disclosure of Protected Health Information (PHI) on behalf of, or providing services to, a covered entity (IEHP). The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

B. First Tier Entity: Any party that enters into a written arrangement with IEHP to provide administrative or health care services for an eligible individual.

C. Downstream Entity: Any party that enters into a Provider agreement with a First Tier Entity to provide health care and administrative services.

D. Contractors: Includes all contracted Providers and suppliers, first tier entities, downstream entities and any other entities involved in the delivery of payment for or monitoring of benefits.

E. Health Care Entity: An individual physician or other health care professional, a hospital, a Provider-sponsored organization, a health maintenance organization, a health insurance plan, or any other kind of health care facility, organization, or plan.

F. Protected Health Information (PHI): All individually identifiable health information, (including genetic information) whether oral or recorded in any form, that relates to the past, present, or future physical or mental health or condition of a Member; the provision of health care to a Member; or the past, present, or future payment for the provision of health care to a Member (45 C.F.R. § 160.103).

1. 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; in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); in employment records held by a Covered Entity in its role as employer; and regarding a person who has been deceased for more than fifty (50) years.
23. **COMPLIANCE**

**B. HIPAA Privacy and Security**

2. PHI generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a health care professional to identify an individual and determine appropriate care.

G. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under 45 C.F.R. Part 164, Subpart E (“Privacy of Individually Identifiable Health Information”) 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 (4) factor objective standard (78 Fed. Reg. at 5642).

1. The nature and extent of protected health information involved (including the types of identifies 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.

5. Breach excludes:

   a. 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 a 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 45 C.F.R. part 164, subpart E.

   b. 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 45 C.F.R. part 164, subpart E.

   c. A disclosure of protected health information where a 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.

**PROCEDURES:**

A. Only entities and their respective staff members with a legitimate business “need to know” may access, use or disclose Member information. This includes all activities related to treatment, payment and health care operations on behalf of IEHP. Each Provider and their
23. COMPLIANCE

B. HIPAA Privacy and Security

respective staff members may only access, use or disclose the minimum information necessary to perform his or her designated role regardless of the extent of access provided to him or her.

B. With respect to system access, Member privacy will be supported through authorization, access, and audit controls (e.g., roles-based access) and should be implemented for all systems that contain identifying Member information. Within the permitted access, a Member-system user is only to access what they need to perform his or her job.

1. Each delegated entity is responsible to perform the security functions and implement the security controls outlined in the attached CPE Delegation Oversight Annual Audit Tool. (See Attachment, “CPE Delegation Oversight Annual Audit Tool” in Section 23)

C. Each entity is responsible for participating in ongoing education regarding Member privacy and Member rights.

D. Each entity is responsible for compliance with these Protected Health Information policies and principles.

E. Permitted Uses and Disclosures

1. Except as otherwise required by law, entities are allowed to release Member information, including PHI, without Member authorization, to IEHP for treatment, payment, or health care operations related to IEHP plans or programs.

2. Activities which are for purposes directly connected with the administration of services include, but are not limited to:
   a. Establishing eligibility and methods of reimbursement;
   b. Determining the amount of medical assistance;
   c. Arranging or providing services for Members;
   d. Conducting or assisting in an investigation, prosecution, or civil or criminal proceeding related to the administration of IEHP plans or programs; and
   e. Conducting or assisting in an audit related to the administration of IEHP plans or programs.

3. PHI must be provided to patients, or their representative if requested, preferably in an electronic format, under HIPAA and the HITECH Act.

4. PHI cannot be sold unless it is being used for public health activities, research or other activities as specified by HIPAA and/or the HITECH Act.

5. HIPAA gives the patient the right to make written requests to amend PHI that you are responsible for maintaining.
23. COMPLIANCE

B. HIPAA Privacy and Security

6. Upon patient request, an accounting of disclosures of PHI, and information related to such disclosures, must be provided to the patient in compliance with 45 CFR Section 164.528.

F. Privacy Practices Notice

1. In accordance with HIPAA 45 CFR §164.520, IEHP provides the “Notice of Privacy Practice” (See Attachment, “Notice of Privacy Practices” in Section 23) to each new Member as follows:
   a. At enrollment and annually thereafter;
   b. Within sixty (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.
   d. 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.

G. Reporting of Unauthorized Access or Disclosures

1. IEHP or Providers must only provide the following required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

2. Reporting of Breaches of Unsecured Protected Health Information Affecting Fewer than five hundred (500) Individuals
   a. For breaches that affect fewer than five hundred (500) individuals, IEHP or Providers must provide the Secretary of the Department of Health and Human Services (DHHS) with notice annually. All notifications of breaches occurring in a calendar year must be submitted within sixty (60) days of the end of the calendar year in which the breaches occurred. This notice must be submitted electronically by completing all information required on the breach notification form which can be found on the DHHS website. A separate form must be completed for every breach that has occurred during the calendar year.

3. Reporting of Breaches of Unsecured Protected Health Information Affecting five hundred (500) or More Individuals:
   a. If a breach affects five hundred (500) or more individuals, IEHP or Providers must provide the Secretary of DHHS with notice of the breach without unreasonable delay and in no case later than sixty (60) days from discovery of the breach. This
23. **COMPLIANCE**

B. **HIPAA Privacy and Security**

notice must be submitted electronically by completing all information required on the breach notification form which can be found on the DHHS website.

b. For all security breaches that require a security breach notification to more than five hundred (500) California residents as a result of a single breach of the security system, IEHP or Providers shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Office of the Attorney General.

c. In addition to notifying the affected Members, IEHP or Providers are required to provide notice to prominent media outlets serving the State or jurisdiction. IEHP will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach and must include the same information required for the individual notice.

4. **Submission of Additional Breach Information to DHHS:**

a. If a breach notification form has been submitted to the Secretary and additional information is discovered, IEHP or Providers may submit an additional form, checking the appropriate box to signal that it is an updated submission. If, at the time of submission of the form, it is unclear how many individuals are affected by a breach, provide an estimate of the number of individuals affected. As this information becomes available, an additional breach report may be submitted as an addendum to the initial report.

5. **Reporting Breaches to the Department of Health Care Services (DHCS):**

a. IEHP must also notify DHCS when a breach occurs that affects a Medi-Cal Member. Notification is provided to the DHCS Privacy Office, Information Security Office and to the Contract Manager within the following timelines:

1) By telephone, e-mail or fax within twenty-four (24) hours of discovery if PHI was or suspected to have been acquired by an unauthorized person.

2) After sending initial notice, IEHP will have seventy-two (72) hours from the date of discovery to provide DHCS with an initial Privacy Incident Report (PIR).

3) Within ten (10) calendar days of discovery of the breach a final, completed PIR will be submitted to DHCS, unless an exception has been obtained from DHCS for additional time needed to complete investigation.

b. It is the expectation of IEHP that entities involved in breaches affecting IEHP DualChoice MediConnect Plan (Medicare – Medicaid Plan) Members notify IEHP within twenty-four (24) hours of discovery if PHI was, or suspected to have been,
23. **COMPLIANCE**

B. **HIPAA Privacy and Security**

acquired by an unauthorized person. In the event that an entity provides notice to DHCS, IEHP should also be notified.

6. Member Breach Notifications

   a. The IEHP Member(s) whose PHI has been breached must be notified in writing of the breach in accordance with CMS and DHHS requirements. IEHP or Providers are required to also notify the affected Member(s) in written form and must be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach. This notification must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected Members should take to protect themselves from potential harm, a brief description of what IEHP and/or Providers are doing to investigate the breach, mitigate the harm and prevent further breaches, as well as IEHP contact information or the contact information of the entity that caused the breach.

7. Reporting Breaches to IEHP

   a. The IEHP Compliance Officer must be notified of any and all unauthorized breaches within the contractual and regulatory timeline requirements stated above. Reports of such breaches may be sent to IEHP using one of the following methods:

      By Mail to:        IEHP Compliance Officer  
                          Inland Empire Health Plan  
                          P.O. Box 1800  
                          Rancho Cucamonga, CA 91729-1800

      By E-Mail to:     compliance@iehp.org

      By Fax to:        (909) 477-8536

      By Compliance Hotline: (866) 355-9038 (for initial notification)

      By Webform:   IEHP.org  Provider Resources – Compliance Tab

H. Corrective Action Subsequent to a Breach

1. Entities must take prompt corrective action to mitigate and correct the cause(s) of unauthorized disclosure/breaches. IEHP requires that a written Corrective Action Plan (CAP) be submitted subsequent to a breach of IEHP Member PHI. A CAP can be submitted:

      By Mail to:       IEHP Compliance Officer  
                          Inland Empire Health Plan  
                          P.O. Box 1800  
                          Rancho Cucamonga, CA 91729-1800
23. **COMPLIANCE**

B. **HIPAA Privacy and Security**

By E-Mail to: compliance@iehp.org

By Fax to: (909) 477-8536

**REFERENCES:**


B. U.S. Dept. of Health and Human Services (DHHS), section 13402(h)(2) of Public Law 111-5 (HITECH ACT).


D. California Health and Safety Code, Section 1280.15.
C. Health Care Professional Advice to Members

APPLIES TO:

A. This policy applies to all IEHP DualChoice Cal MediConnect Plan (Medicare – Medicaid Plan) Members.

POLICY:

A. IEHP and contracted partners shall not prohibit or restrict a health care professional acting within their professional scope of work and licensure, from advising or advocating on behalf of a Member whom they are caring for.

PROCEDURE:

A. A health care professional shall be able to give advice or advocate for a Member regarding the Member’s:
   1. Health Status;
   2. Medical Care;
   3. Treatment options, which include:
      a. Self-administered alternative treatments; and
      b. Adequate information to make a decision against treatment options.
   4. Risks and benefits of such treatments or non-treatments;
   5. Right to refuse treatment; and
   6. Right to express preferences about future treatment decisions.

B. A health care professional shall provide to a Member treatment options, including the option of no treatment, in a culturally competent manner. A health care professional shall ensure a Member with a disability has effective communications, with participants throughout the health system, in making decisions regarding treatment options.

C. IEHP shall inform Members of their right to refuse treatment and information regarding advance directives in accordance with Policy 7D, “Advance Health Care Directive.”

D. If a contracted provider violates the terms of this policy, they will be subject to contract termination.

REFERENCE:

23. COMPLIANCE

C. Health Care Professional Advice to Members
## 23. COMPLIANCE

Attachments

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>POLICY CROSS REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPE Delegation Oversight Annual Audit Tool</td>
<td>23C</td>
</tr>
<tr>
<td>IEHP Vendor Code of Conduct</td>
<td>23C, 24E, 24F</td>
</tr>
<tr>
<td>Notice of Privacy Practices</td>
<td>23D</td>
</tr>
</tbody>
</table>
### Delegation Oversight Annual Audit Tool 2019

**Compliance**

**HIPAA PRIVACY RULE**

(45 CFR Part 160 and Subparts A, D & E of Part 164)

#### Scoring Key:
- 0 = non-compliant
- 1 = partially compliant
- 2 = fully compliant
- N/A = not applicable

**Instructions:** Review each of the requirements below, and enter an “X” in the appropriate column for level of compliance. Enter comments to explain areas of non-compliance, and actions planned/taken to address the deficiency with expected date of completion. Please indicate page number and section number for any supporting documentation in the provided Supporting Documentation Column.

---

### A. Confidentiality of Member Information

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Supporting Documentation</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Regarding confidentiality of Member medical records and other Member Protected Health Information (PHI); including electronic PHI (ePHI).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>2. That protect against unauthorized or inadvertent disclosure of information to any individual, including the delegate’s own employees or contractors, who do not have an identifiable need for the information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>a. Authorization and/or Supervision: has procedures for the authorization and/or supervision of workstations, workforce members, and contractors who work with PHI/ePHI or in locations where it might be accessed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>b. Workforce Clearance Procedure: has procedures to determine that the access of a workstation by contractors and/or workforce to PHI/ePHI is appropriate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>c. Termination Procedures: has procedures for terminating access to PHI/ePHI when the employment of a workforce member or contractor ends or access to ePHI is inappropriate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>3. That releases Member PHI only in accordance with Federal and State laws, court orders, or subpoenas, which includes release of Member information to a Member when requested by that Member. This includes providing access to IEHP Members (upon reasonable notice and during delegate's normal business hours) to their PHI in the delegate's Designated Record Set in accordance with 45 CFR 164.524.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>4. That ensures its contracts document that the delegate requires sub-contractors or agents to whom the delegate provides PHI and/or ePHI to agree to the same restrictions and conditions that apply to the delegate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>5. To prevent, detect, contain, and correct security violations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td><strong>COMMENTS:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Requirements Section A**

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average</strong></td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### B. General Security Controls

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Supporting Documentation</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Has policies and procedures that ensures all persons that work with PHI sign a confidentiality statement, prior to PHI access and renew statement annually; statement to include, 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 IEHP PHI(ePHI).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>2. Maintains evidence that a confidentiality statement is signed, prior to PHI access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td>3. Maintains evidence that all persons that work with PHI sign a confidentiality statement annually.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td><strong>COMMENTS:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Requirements Section B**

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average</strong></td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### C. Record Retention

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Supporting Documentation</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Documenting the record retention policy is no less than ten (10) years for Medicare related medical records data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Include page and section numbers where applicable)</td>
<td></td>
</tr>
<tr>
<td><strong>COMMENTS:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Requirements Section C**

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average</strong></td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### D. Paper Document Controls

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Supporting Documentation</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COMMENTS:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Requirements Section D**

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average</strong></td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

---
1. Documenting that PHI in paper form shall not be left unattended at any time unless it is locked up. Applies to work and non-work related settings (i.e., home office, transportation, travel, fax machines, copy machines etc.).

2. That ensures visitors to areas where PHI is contained shall be escorted and PHI shall be kept out of sight while visitors are in the area, unless they are authorized to review PHI.

3. That requires PHI to be destroyed through confidential means, such as cross-shredding or pulverizing, in a manner that prevents reconstruction of contents. There must be evidence of PHI destruction in accordance with HIPAA if an external vendor is utilized.

4. Stating that PHI is not to be removed from the delegate's premises except for routine business purposes.

5. That ensures faxes contain a confidentiality statement notifying persons receiving faxes in error to destroy them.

6. For the mailing of PHI only by secure methods. Large volume mailings of IEHP PHI shall be mailed by a secure, bonded courier with signature required on receipt. Disks and transportable media sent through the mail must be encrypted.

7. That ensures shredder bins are available for destruction of documents with PHI, clearly marked, and not filled to overflowing.

COMMENTS:

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Total Requirements Section D**

**E. Documentation and Accounting of Disclosures**

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

**F. Notification and Investigation of Breach and Security Incident**

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

**G. Actions to Mitigate Breach Risk and Security Incidents**
1. Has policies and procedures demonstrating that prompt corrective action to mitigate any risks or damages involved with the breach or security incident are taken.

2. Has policies and procedures that ensures corrective action in response to a breach or security incident is documented and monitored for effectiveness.

3. Has policies and procedures for disciplinary actions related to breaches or security incidents caused by employee and/or subcontractor carelessness and/or disregard of HIPAA and HITECH requirements.

4. Has policies and procedures to indicate that appropriate corrective actions are taken to mitigate any risk or damages from a breach or security incident.

**Comments:**

### Total Requirements Section G

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### H. HIPAA and HITECH Training for Staff

<table>
<thead>
<tr>
<th>The delegate:</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Supporting Documentation (Include page and section numbers where applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Has policies indicating that all staff members (including physicians) are required to receive HIPAA and HITECH training upon initial employment and annually.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Refer to Tab 5, File Review - P &amp; S Training, Section C</td>
</tr>
<tr>
<td>2. Maintains evidence that staff members (including physicians) are required to receive HIPAA and HITECH training upon initial employment and annually.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Refer to Tab 5, File Review - P &amp; S Training, Section D</td>
</tr>
<tr>
<td>3. Maintains evidence that staff members (including physicians) are required to receive HIPAA and HITECH training annually.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Has policies indicating that HIPAA and HITECH training materials include the following:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. mechanisms in place for staff members to report suspected breaches, anonymously if they so choose;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. policy on non-retaliation for reporting suspected breaches.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Comments:**

### Total Requirements Section H

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### Total Requirements HIPAA Privacy Rule

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Delegation Oversight Annual Audit Tool 2019

HIPAA SECURITY RULE
(45 CFR Part 160 and Subparts A & C of Part 164)

Medical Management System(s): ________________________________

Scoring Key: 0 = non-compliant; 1 = partially compliant; 2 = fully compliant; N/A = not applicable

Instructions: Review each of the requirements below, and enter an “X” in the appropriate column for level of compliance. Enter comments to explain areas of non-compliance, and actions planned/taken to address the deficiency with expected date of completion. Please indicate page number and section number for any supporting documentation in the provided Supporting Documentation Column.

### A. Administrative Safeguards (45 CFR § 164.308)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Security Awareness and Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Refer to Tab 5: File Review - P &amp; S Training, Section E</td>
</tr>
</tbody>
</table>

#### The delegate:

1. Maintains evidence that security awareness and training is conducted annually for all members of its workforce (including management).

2. Has policies and procedures that require the implementation of security reminders (e.g., notices in printed or electronic form, monthly meetings, posted reminders, agenda items on monthly meetings, etc.).

   - a. guarding against, detecting, and reporting malicious software;
   - b. computer systems (desktop computer, laptop, tablet device, smart phones) used to access, store and/or transmit ePHI have anti-malware software installed and up to date.

3. Has policies and procedures related to the Protection from Malicious Software that address:

   - a. guarding against, detecting, and reporting malicious software;
   - b. anti-malware software installed and up to date.

4. Has policies and procedures related to log-in monitoring. Procedures must address monitoring log-in attempts and reporting discrepancies.

5. Has policies and procedure related to password management. Procedures must address creating, changing, and safeguarding passwords (i.e. complex password requirements).

6. Enforces their password management policy.

**Provide documentation or screenshots showing policy is enforced through system administration management interface \ console. Alternatively, system(s) walkthrough will be scheduled.**

### B. Physical Safeguards (45 CFR § 164.310)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Facility Access Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### The delegate:

Has policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. The delegate:

1. Facility security plan: has policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

2. Access control and validation procedures: has procedures to control and validate a person’s access to facilities based on their role or function, including visitors.

3. Maintenance records: has policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

**COMMENTS:**
### B. Device and Media Controls

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>The delegate:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Disposal:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. has policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. computer systems (desktop computer, laptop, tablet device, smart phones) used to store ePHI that do not use whole disk encryption must have the hard drives &quot;wiped&quot; before being donated, thrown away or otherwise discarded;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Media re-use:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>has procedures for removal of ePHI from electronic media before the media are made available for re-use.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Accountability:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>maintains a record of the movements of hardware and electronic media and any person responsible therefore.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Data backup and storage:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>creates a retrievable, exact copy of ePHI, when needed, before movement of equipment.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Total Requirements Section B

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### C. Technical Safeguards (45 CFR § 164.310)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>The delegate:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has implemented technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. The delegate's has policies that require:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Unique user identification: assigns a unique name and/or number for identifying and tracking user identity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Automatic logoff: has electronic procedures that terminate an electronic session after a predetermined time of inactivity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. The delegate maintains evidence that an authorization process is in place for the granting of access to PHI to workforce members.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. A process for limiting administrator access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has implemented the following controls for its existing electronic health record (EHR):</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Role based access;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Unique user IDs;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has implemented controls to ensure electronic PHI (ePHI) stored on laptops and removable storage devices (e.g. externally connected USB, Fire wire, eSATA hard drives, USB thumb or flash drives, recordable CD/DVDs, etc.) is encrypted.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Screen shots of management console or screenshots of encryption application installed on, at a minimum, on laptops, and removable drives.</td>
</tr>
</tbody>
</table>

### COMMENTS:

#### B. Access Control

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>The delegate:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has implemented technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. The delegate's has policies that require:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Unique user identification: assigns a unique name and/or number for identifying and tracking user identity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Automatic logoff: has electronic procedures that terminate an electronic session after a predetermined time of inactivity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. The delegate maintains evidence that an authorization process is in place for the granting of access to PHI to workforce members.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. A process for limiting administrator access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has implemented the following controls for its existing electronic health record (EHR):</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Role based access;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Unique user IDs;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### COMMENTS:

#### B. Audit Controls

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>The delegate:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintains procedures which indicate the implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI; includes security event monitoring.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. User Access to system is logged by user id, IP address, date and time.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provide screen shots of existing system logs. Alternatively, a system(s) walkthrough can be scheduled.</td>
</tr>
<tr>
<td>3. Changes to member records are logged and include the author of the changes as well as the change that was made.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provide screen shots of existing system logs. Alternatively, a system(s) walkthrough can be scheduled.</td>
</tr>
<tr>
<td>4. Audit Logs are retained for 10 years.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. System Security Review: All systems process and/or storing IEHP PHI must have at least an annual system security review. Reviews must include administrative and technical vulnerability scanning tools.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Log Reviews: All systems processing and/or storing IEHP PHI must have a routine procedure in place to review system logs for unauthorized access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**C. Integrity**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Supporting Documentation</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The delegate</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Mechanisms to authenticate ePHI: has electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Anti-virus software: Ensures all workstations, laptops and other systems that process and/or store IEHP PHI have a commercial third-party anti-virus software solution.</td>
<td></td>
<td></td>
<td></td>
<td>Provide screen shots of management console or screenshots of software installed on the laptops, workstations, and other systems. Alternatively, a system(s) walkthrough can be scheduled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Patch Management: Ensures All workstations, laptops and other systems that process and/or store IEHP data have security patches applied and up-to-date.</td>
<td></td>
<td></td>
<td></td>
<td>Provide a recent report or screenshots of patch management system console showing current patch status on desktops and servers. Alternatively, a system(s) walkthrough can be scheduled.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**COMMENTS:**

**D. Person or Entity Authentication**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Supporting Documentation</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The delegate</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintains policies and procedures to verify that a person or entity seeking access to ePHI is the one claimed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**COMMENTS:**

**E. Transmission Security**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>N/A</th>
<th>Supporting Documentation</th>
<th>Comment/Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The delegate</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintains policy and procedures that ensure technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Policies and Procedures shall require:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Integrity controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. The application of security to computer operating systems and applications that access, store, and/or transmit ePHI.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Computer systems (desktop computer, laptop, tablet device, smart phones) used to access, store and/or transmit ePHI have a firewall installed and turned on to block unauthorized connections into the computer system from the internet.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Remote Access: any remote access to IEHP PHI must be executed over an encrypted method using a vendor product specified on CSSI.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Remote access must be limited to minimum necessary and least privilege principles.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Encryption: has a mechanism to encrypt ePHI whenever deemed appropriate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Transmits all email that include IEHP PHI via an encrypted method using a solution from a vendor product specified on the CSSI.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provide evidence of email encryption capability (send email to <a href="mailto:DGComplianceAM@iehp.org">DGComplianceAM@iehp.org</a> with the subject line &quot;2019 DO Audit of &lt;insert the name of your organization&gt;&quot; or provide screen shots that demonstrate encryption capability. Alternatively, a system(s) walkthrough can be scheduled.</td>
<td></td>
</tr>
</tbody>
</table>

**COMMENTS:**

---

**Total Requirements Section C**

<table>
<thead>
<tr>
<th>Requirement Met</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average</strong></td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

---

**Total Requirements HIPAA SECURITY RULE**

<p>| Requirement Met | 0 | 0 | 0 | 0 |</p>
<table>
<thead>
<tr>
<th>Average</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
</tr>
</thead>
</table>
Vendor Code of Conduct

Commitment, Mission, Core Values and Code of Conduct

Commitment
IEHP is firmly committed to complying with its legal, ethical and contractual obligations under all State and Federal programs, laws, regulations, directives and transmittals applicable to Medi-Cal, Medicare, Healthy Kids and other lines of business in which IEHP may choose to participate. As a result, any entity doing business with IEHP, including vendors, business associates, first tier, downstream and related entities (collectively referred to as Vendors), is expected to understand and comply with these obligations.

IEHP Mission
To organize and improve the delivery of quality, accessible and wellness based healthcare services for our community.

IEHP Core Values
Health and Quality Before Costs; Think and Work Lean; Team Culture; Partner with Providers; Stewardship of Public Funds.

IEHP Code of Business Conduct and Ethics
IEHP expects its employees and Vendors to work together in an ethical and professional manner that promotes public trust and confidence in the integrity of IEHP. The IEHP Code of Business Conduct and Ethics is meant to provide guidance about the compliance culture at IEHP and the role that each Vendor and employee plays in building and preserving that culture. IEHP expects that all Vendors will implement similar standards of conduct for their organization. The IEHP Code of Business Conduct and Ethics can be found at: https://ww3.iehp.org/en/providers/educational-opportunities/code-of-business-conduct-and-ethics/.

Compliance with Laws and Regulations
IEHP is committed to conducting all activities and operations in compliance with applicable laws and regulations. By making it the responsibility of all Vendors doing business with IEHP to regulate compliance with our strict ethical standards and commitment to comply with legal responsibilities, we can continue to maintain the highest level of moral, ethical and legal standards in conducting our business. Vendors working directly or indirectly on government contracts (e.g., Medicare, Medi-Cal, etc.) have a special obligation to know and comply with all the terms of the government contract.

False Claims Act
The State and Federal False Claims Acts prohibit presenting false or fraudulent claims to the government for payment, making any false statements or representations or doing business with debarred individuals or entities. Vendors shall comply with all requirements of both the State and Federal False Claims Acts in its billing practices to IEHP. In addition, Vendors must cooperate fully with any government and audit-related requests for information.
**Compliance with Laws and Regulations continued…**

**Anti-Kickback Statute**
The Anti-Kickback Statute prohibits a person or entity from knowingly or willfully soliciting, receiving, offering or paying for referrals for items or services which may be reimbursed by a Federal health care program. A Federal health care program is defined as any plan or program that provides health benefits, whether directly or indirectly, through insurance which is funded by the United States Government or any State health care program. Therefore, the Anti-Kickback Statute applies both to Medicare and Medi-Cal. Vendors shall comply with all requirements of the Anti-Kickback law in its business practices.

**Stark Law**
The Stark Statute prohibits a physician from referring Medicare patients for designated health services to an entity with which the physician, or immediate family member, has a financial relationship, unless an exception applies. This law also prohibits the designated health services entity from submitting claims to Medicare for those services resulting from a prohibited referral. Vendors shall comply with all requirements of the Stark law for all referral and billing practices.

**Whistleblower Protections**
The rights of whistleblowers include protections against demotion, suspension, discharge, threats or threatening behavior, harassment or other discrimination in the terms and conditions of employment by the employer because of lawful acts done by the employee on behalf of the employee or others in disclosing information to the government. IEHP requires Vendors to have policies in place to protect employees who disclose actual or reasonably suspected violations or provide assistance to the government in pursuing an action as allowed under both the Deficit Reduction Act and the False Claims Act.

**Compliance Training**
IEHP requires all Vendors to provide Compliance Training to their employees and vendors within the first 90 days of employment and annually thereafter. Compliance Training should include general compliance issues, fraud, waste and abuse (FWA), and privacy related matters.

**Privacy and Security**

**Confidentiality / Data Integrity**
IEHP recognizes the importance of its Members’ right to confidentiality and implements policies and procedures to ensure its Members’ confidentiality rights, including protected health information (PHI). PHI is information that both identifies a Member and relates to their past, present, or future health or condition, provision of care or payment for care. IEHP has a responsibility to protect the confidentiality of any data that is entrusted to it by its Members, Vendors and Regulatory Agencies. This data may include PHI and other proprietary and confidential information. Vendors whose work requires the use and disclosure of PHI are considered Business Associates and must execute a Business Associate Agreement in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and any ensuing amendments. Vendors shall safeguard IEHP Member identity, eligibility, social security, medical information and other confidential information in accordance with applicable laws.
**Member Rights**

**Member Choice, Access to Health Care Services, Continuity of Care**
IEHP Members deserve to be treated with respect and to experience the kind of customer service that each one of us expects from each other. Vendors shall comply with IEHP policies and procedures and applicable laws governing Member choice, access to health care services and continuity of care. Every Member encounter with a Vendor is an opportunity to demonstrate excellent customer service.

**Accommodations and Accessibility**
Vendors shall provide culturally, linguistically and sensory appropriate services to IEHP Members to ensure effective communication regarding diagnosis, medical history and treatment and health education. In addition, Vendor facilities shall adhere to the requirements of the Americans with Disabilities Act of 1990 by providing access for Members with disabilities.

**Non-Discriminatory / Non-Retaliation Policy**
IEHP complies with all applicable anti-discrimination laws. Vendors shall not discriminate on the basis of race, color, religion, national origin, age, gender, sexual orientation, physical or mental disability or any other classification protected by law. In addition, IEHP has a zero tolerance retaliation policy. IEHP prohibits retaliation against any individual who reports discrimination, harassment, compliance concerns or participates in an investigation involving such reports. Individuals are encouraged to report compliance issues or suspected issues without fear of intimidation or retaliation including, but not limited to, fraud, waste and abuse, privacy issues and other issues of non-compliance. Any information reported will be treated as confidential to the extent possible, without failing to fulfill legal obligations.

**Grievance and Appeals Processes**
Vendors shall ensure that IEHP Members are informed of their grievance and appeal rights including, the State Hearing process, through publications and other communications in accordance with IEHP policies and procedures and applicable laws.

**Business Relationships**

**Conflict of Interest**
Vendors shall comply with all applicable Federal, State and local laws and regulations pertaining to conflict of interest laws, including IEHP’s Conflict of Interest Policy. A conflict of interest typically presents itself in the form of a personal or financial gain for an individual or entity that could possibly corrupt the motivation of that individual or entity. Vendors should avoid any business, activity or situation which may possibly constitute a conflict of interest and the interests of IEHP. If a Vendor or its employee has a personal or other relationship with an IEHP employee that might represent a conflict of interest, the Vendor should disclose this information to IEHP.

**Fair Competition**
IEHP competes fairly in the marketplace and conducts its business with integrity. Interactions, including those involving Vendors, must always be fair and mindful of ethical business practices. IEHP strictly adheres to all Federal and State antitrust laws. Similarly, Vendors are expected to comply with all antitrust and fair business practice laws.
Business Relationships continued...

Gifts
IEHP discourages its Vendors from providing personal gratuities, gifts, favors, services, entertainment or other business courtesies to IEHP employees, regardless of value. All decisions and actions regarding external relationships and purchasing must be based on proper business considerations and not influenced in any way by personal obligations. IEHP is a public entity and required to comply with the rules set forth by the California Fair Political Practices Commission. A Vendor may not accept gifts, entertainment or any other personal favor or preferential treatment to or from anyone with whom IEHP has, or is likely to have, any business dealings.

Exclusionary Screening / Ineligible Vendors
IEHP has a screening process to identify individuals and entities that appear on the Office of Inspector General (OIG) exclusion database, General Services Administration System for Award Management (SAM) and Medicare Opt-Out List and/or Medi-Cal Suspended and Ineligible Provider List before initial appointment, contracting, credentialing, payments and/or hiring and monthly thereafter. IEHP requires that Vendors develop and implement similar standards for screening of their employees and FDRs. IEHP will not do business with any Vendor if it or any of its employees are, or become excluded by, debarred from, or ineligible to participate in any Federal or State program. Vendors must disclose to IEHP if they, or any of their employees, are currently suspended, debarred or otherwise ineligible to participate in any Federal or State program or become suspended, debarred or otherwise ineligible after contracting with IEHP.

Compliance Program Reporting

Reporting Potential Violations
If any Vendor becomes aware of any issue of non-compliance, including potential fraud, waste and abuse, privacy incident, a violation of a legal or ethical obligation or any unfair or improper treatment of an IEHP Member, they must immediately report the matter to the IEHP Compliance Department so that it can be investigated. IEHP holds all entities doing business with IEHP responsible for carrying out and monitoring compliance with this commitment. IEHP will conduct a fair, impartial and objective investigation into concerns brought to its attention and will take appropriate action to correct any violations or issues. Investigative findings that meet State and/or Federal criteria for additional investigation are referred to the appropriate State and/or Federal entity.

Modes of Reporting
Persons making a report to IEHP’s Compliance Department may do so anonymously. Reports may be submitted by:

- **Phone:** IEHP Compliance Hotline
  (866) 355-9038
- **Email:** compliance@iehp.org
- **Fax:** (909) 477-8536
- **Mail:** IEHP Compliance Officer
  P.O. Box 1800
  Rancho Cucamonga, CA 91729-1800
Message From
INLAND EMPIRE HEALTH PLAN (IEHP)

Notice of Privacy Practices
Effective: April 14, 2003
Revised: January 1, 2019

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

IEHP provides health care to you through Federal, State and Commercial programs. We are required by state and federal law to protect your health information. And we must give you this Notice that tells how we may use and share your information and what your rights are.

Your information is personal and private.
We receive information about you from Federal, State and local agencies after you become eligible and enroll in our health plan. We also receive medical information from your doctors, clinics, labs, and hospitals in order to approve and pay for your health care.

CHANGES TO NOTICE OF PRIVACY PRACTICES
IEHP must obey the Notice currently in effect. We reserve the right to make any revised or changed notice effective for information we already have and for information that we receive in the future. If we do make changes we will revise this Notice and send it to you right away.

How We May Use and Share Information About You
Your information may be used or shared by IEHP only for treatment, payment and health care operations associated with the particular program in which you are enrolled. The information we use and share includes, but is not limited to:
• Your name,
• Address,
• Personal facts,
• Medical care given to you, and
• Your medical history.

Some actions we take when we act as your Health Plan include:
• Checking your eligibility, enrollment, and amount of medical aid
• Approving, giving, and paying for health care services
• Investigating or prosecuting cases (like fraud)
• Checking the quality of care that you receive
• Coordinating the care you receive
Some examples of why we would share your information with others involved in your health care:

1. **For treatment:** You may need medical treatment that requires us to approve care in advance. We will share information with doctors, hospitals and others in order to get you the care you need.

2. **For payment:** IEHP reviews, approves, and pays for health care claims sent to us for your medical care. When we do this, we share information with the doctors, clinics, and others who bill us for your care. And we may forward bills to other health plans or organizations for payment.

3. **For health care operations:** We may use information in your health record to judge the quality of the health care you receive. We may also use this information in audits, fraud and abuse investigations, planning, and general administration.

We may also contact you to provide information about other health-related benefits and services that may be of interest to you, such as health education programs and management of certain health conditions.

**Other Uses For Your Health Information**

1. Sometimes a court will order us to give out your health information. We will also give information to a court, investigator, or lawyer if it is about the operation of one of the other programs. This may involve fraud or actions to recover money from others, when the Federal, State, Commercial entity or IEHP has paid your medical claims.

2. You or your doctor, hospital, and other health care providers may appeal decisions made about claims for your health care. Your health information may be used to make these appeal decisions.

3. We may also share your health information with agencies and organizations, which check how our health plan is providing services.

4. We must share your health information with the federal government when it is checking on how we are meeting privacy rules.

**When Written Permission is Needed**

If we want to use your information for any purpose not listed above, we must get your written permission. If you give us your permission, you may take it back in writing at any time.

**What Are Your Privacy Rights?**

You have the right to ask us not to use or share your protected health care information in the ways described above. We may not be able to agree to your request.

You have the right to ask us to contact you only in writing or at a different address, post office box, or by telephone. We will accept reasonable requests when necessary to protect the safety of your information.

You and your personal representative have the right to inspect and get a paper or electronic copy of your health information. You will be sent a form to fill out and may be charged a fee for the costs of copying and mailing records. (We may keep you from seeing certain parts of your records for reasons allowed by law.)

You have the right to ask that information in your records be amended if it is not correct or complete. We may refuse your request if:

- The information is not created or kept by IEHP, or
- We believe it is correct and complete.
If we don't make the changes you ask, you may ask that we review our decision. You may also send a statement saying why you disagree with our records and your statement will be kept with your records.

You have the right to be notified of a breach of unsecured protected health information in the event that you are affected by the breach.

You have the right to restrict certain disclosures of protected health information to IEHP where you pay, or another person on your behalf pays, out of pocket in full for the health care item or service.

You have the right to receive an account of instances where your protected health information was shared.

### IMPORTANT

IEHP DOES NOT HAVE COMPLETE COPIES OF YOUR MEDICAL RECORDS. IF YOU WANT TO LOOK AT, GET A COPY OF, OR CHANGE YOUR MEDICAL RECORDS, PLEASE CONTACT YOUR DOCTOR OR CLINIC.

When we share your health information you have the right to request a list of:
- Whom we shared the information with,
- When we shared it,
- For what reasons, and
- What information was shared.

You have a right to request a paper copy of this Notice of Privacy Practices.
You can also find this Notice on our website at: www.iehp.org

**How do you Contact us to Use Your Rights?**

If you want to use any of the privacy rights explained in this Notice, please write us at:

**IEHP Director of Compliance**
INLAND EMPIRE HEALTH PLAN
P.O. Box 1800
Rancho Cucamonga, CA 91729
Email: compliance@iehp.org

Or, you can call IEHP Member Services at 1-800-440-IEHP (4347); TTY/TDD users should call 1-800-718-4347.

**Complaints**

If you believe that we have not protected your privacy and wish to complain, you may file a complaint by writing:

**INLAND EMPIRE HEALTH PLAN**
P.O. Box 1800
Rancho Cucamonga, CA 91729

Or, you can call IEHP Member Services at 1-800-440-IEHP (4347); TTY/TDD users should call 1-800-718-4347.

Or, you may contact the agencies below:

**Privacy Officer**
c/o: Office of HIPAA Compliance

Department of Health Care Services
P.O. Box 997413, MS 4722
Sacramento, CA 95899-7413
Email: Privacyofficer@dhcs.ca.gov
Telephone: (916) 445-4646
Fax: (916) 440-7680
Use Your Rights Without Fear

IEHP cannot take away your health care benefits or do anything to hurt you in any way if you choose to file a complaint or use any of the privacy rights in this Notice.

IEHP has always been committed to protecting Members’ privacy and maintaining the confidentiality of their personal and medical information in all settings in accordance with and in compliance with HIPAA and all other state and federal laws. All IEHP employees are required to have education and training upon hire and annually thereafter about ways to protect your health information from being looked at and/or talked about by others who are not a part of your healthcare delivery system. We have, and enforce, policies about limiting building access and visitors to IEHP. Electronic records are protected by administrative, physical and technical safeguards. Our Business Associates are required to have the same privacy protections that IEHP has in place.

Questions

If you have any questions about this Notice and want further information, please contact the IEHP Privacy Officer at the address and phone number listed on page 3.
Inland Empire Health Plan (IEHP) complies with applicable Federal civil rights laws and does not discriminate on the basis of race, color, national origin, age, disability, or sex. IEHP does not exclude people or treat them differently because of race, color, national origin, age, disability, or sex.

IEHP:

- Provides free aids and services to people with disabilities to communicate effectively with us, such as:
  - Qualified sign language interpreters
  - Written information in other formats (large print, audio, accessible electronic formats, other formats)
- Provides free language services to people whose primary language is not English, such as:
  - Qualified interpreters
  - Information written in other languages

If you need these services, contact IEHP Member Services at 1-800-440-4347 (TTY: 1-800-718-4347).

If you believe that IEHP has failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance with:

Civil Rights Coordinator
Inland Empire Health Plan
10801 Sixth Street, Suite 120
Rancho Cucamonga, CA 91730
**Telephone:** 1-800-440-4347 (TTY: 1-800-718-4347)
**Fax:** 1-909-890-5748
**Email:** CivilRights@iehp.org

You can file a grievance in person or by mail, fax, or email. If you need help filing a grievance the Civil Rights Coordinator is available to help you.

You can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, electronically through the Office for Civil Rights Complaint Portal, available at https://ocrportal.hhs.gov/ocr/portal/lobby.jsf, or by mail or phone at:

U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201
1-800-368-1019, 800-537-7697 (TDD)

DISCRIMINACIÓN ES UN ACTO CONTRA LA LEY

Inland Empire Health Plan (IEHP) cumple con las leyes Federales de derechos civiles aplicables y no discrimina por motivos de raza, color, nacionalidad, edad, discapacidad o sexo. IEHP no excluye a las personas ni las trata de forma diferente debido a su raza, color, nacionalidad, edad, discapacidad o sexo.

IEHP:
- Proporciona asistencia y servicios gratuitos a personas con discapacidad para que se comuniquen de manera eficaz con nosotros, como los siguientes:
  - Intérpretes de lenguaje de señas calificados
  - Información escrita en otros formatos (letra grande, audio, formatos electrónicos accesibles, otros formatos)
- Proporciona servicios lingüísticos gratuitos a personas que prefieren comunicarse en un idioma diferente al inglés, como los siguientes servicios:
  - Intérpretes calificados
  - Información escrita en otros idiomas

Si necesita recibir estos servicios, comuníquese con Servicios para Miembros de IEHP al 1-800-440-4347 (TTY: 1-800-718-4347).

Si considera que IEHP no le proporcionó estos servicios o lo discriminó de otra manera por motivos de raza, color, nacionalidad, edad, discapacidad o sexo, puede presentar una queja formal ante el Coordinador de Derechos Civiles:

Civil Rights Coordinator
Inland Empire Health Plan
10801 Sixth Street, Suite 120
Rancho Cucamonga, CA 91730

Teléfono: 1-800-440-4347 (TTY: 1-800-718-4347)
Fax: 1-909-890-5748  Correo electrónico: CivilRights@iehp.org

Puede presentar una queja formal en persona o por correo postal, fax o correo electrónico. Si necesita ayuda para hacerlo, el Coordinador de Derechos Civiles está a su disposición para ayudarle.

También puede presentar una queja de derechos civiles ante la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de los Estados Unidos de manera electrónica a través del Portal de Quejas de la Oficina de Derechos Civiles, disponible en https://ocrportal.hhs.gov/ocr/portal/lobby.jsf, o bien, por correo postal a la siguiente dirección o por teléfono a los números que figuran a continuación:

U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201
1-800-368-1019, 800-537-7697 (TDD)

DISCRIMINATION IS AGAINST THE LAW
LA DISCRIMINACIÓN ES UN ACTO CONTRA LA LEY

ARABIC

بقوانين الحقوق المدنية وفقاً للمعايير المعمول بها ولا يميز على أساس العرق أو الجنس أو الجنسية أو اللغة. IEHP يلتزم بموجب سياسة IEHP تم التحديد أن اللغة، فإن خدمات المساعدة اللغوية تتوفر لك بالمجان. اتصل برقم 4347-440-800-1 (رقم هاتف الصم والبكم): 1-800-718-4347

ARMENIAN

IEHP-ի համարում է, որ բազմաթիվ պետությունների, կողմերի, զատկից զատկեր, զատկերի պարունակությունների և այլ դերում անցկացվող գործումը չի պահանջում կանոնավոր սպասարկություն և այլ անձագնություն պահպանելու եղանակի: Մասնակցեք 1-800-440-4347 ՏՏԸ (հեռախոս) 1-800-718-4347:

CHINESE

遵守適用的聯邦民權法律規定，不因種族，膚色，民族血統，年齡，殘障或性別而歧視任何人。 注意：如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 1-800-440-4347 （TTY：1-800-718-4347）。

Farsi

از قوانین حقوق مدنی مربوط به تبعیض مبنی بر اساس نژاد، رنگ پوست، اصلیت ملیتی، سن، ناتوانی یا جنسیت افراد باید قابل قبول باشد. IEHP نظارت بر اصول می‌کند. توجه: اگر به زبان فارسی گفتگو می‌کنید، تسهیلات زبانی بصورت رایگان برای شما فراهم می‌گردد. با تاکسی به‌بازار گردد. (TTY: 1-800-718-4347) 1-800-440-4347

HINDI

IEHP नागरिक अधिकार का पालन करता है और जाति, रंग, राष्ट्रीय रूप, आय, विकलांगता, या लिंग के आधार पर भेदभाव नहीं करता है। ध्यान दें: यदि आप हिन्दी बोलते हैं तो आपके लिए सुप्त में भाषा सहायता सेवाएं उपलब्ध हैं। 1-800-440-4347 (TTY: 1-800-718-4347) पर कॉल करें।

HMONG

IEHP ua raws cov kev cailij choj pej xeem uas yuam siv ntawm Tsom Fww Teb Chaw (Federal civil rights laws) thib tsis muaj kev ntxub ntxaug vim yog ihhom neeg, cev nqajj tawv, neeg keeb kwm hauv lub teb chaws, hnuv nyoog laus hluas, kev tsis taus, los sis txiv neeg los yog poy niam.


JAPANESE

IEHP は適用される連邦公民権法を遵守し、人種、肌の色、出身国、年齢、障害または性別に基づく差別をいたしません。注意事項：日本語を話される場合、無料の言語支援をご利用いただけます。1-800-440-4347（TTY:1-800-718-4347）まで、お電話にてご連絡ください。

KHMER

IEHP ប្រកួតពិភពប្រជាជនពិភពលោកត្រូវបានស្គាល់ដោយនូវប្រយោគជាតិសាស្រ្តអិនី.amazonaws ដូចជា ការមិនលើករក្សានូវ ហិរញ្ញវត្ថុ និងការមិនទទួលបញ្ហាច្រើន ដោយស្វែងរកច្បាប់ (Khmer) យ៉ាងស្រស់ស្ត្រីអំពីអ្នកប្រជាជន 1-800-440-4347 (TTY: 1-800-718-4347)