23. COMPLIANCE

A. Monitoring of First Tier and Downstream Entities

APPLIES TO:

A. This policy applies to all IEHP DualChoice (HMO D-SNP) First Tier and Downstream Entities (FTEs).

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 and Downstream Entities (FTEs). Further, IEHP is responsible for maintaining compliance with applicable State and Federal requirements.[1,2,3,4,5]

   1. The terms and conditions set forth in contracts with FTEs 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 FTEs, as appropriate. IEHP monitors FTE performance on an ongoing basis and will implement corrective actions and revoke delegation of duties if it determines that an FTE is unable or unwilling to carry out its responsibilities.

DEFINITIONS:

A. First Tier Entity - 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.[6,7]

B. 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 tier entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services.[8]

[1] Title 42 Code of Federal Regulations (CFR) §422.503(b)(4)(vi)(F), 422.504(i), 423.504(b)(4)(vi)(F), 438.230(b)
[2] Medicare Managed Care Manual, Chapter 9 and 21, "Compliance Program Guidelines," Section 40
[3] 22 CFR §§ 51000-53999
[4] California Welfare and Institutions Code (Welf. & Inst. Code), §§14100-14458
[5] Knox-Keene Health Care Service Plan Act of 1974, §1340
[6] Medicare Managed Care Manual, Chapter 9 and 21, "Definitions," Section 20
[7] 42 C.F.R. § 423.501
[8] Ibid.

23. COMPLIANCE

A. Monitoring of First Tier and Downstream Entities

PURPOSE:

A. The purpose of this policy is to ensure that FTEs and Downstream Entities are compliant with meeting the terms and conditions of regulatory elements as established by Centers for Medicare & Medicaid Services (CMS), the State of California, other governmental entities, and IEHP.

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

C. The Compliance Department enforces the compliance program by ensuring all regulatory requirements and policies and procedures are adhered.

PROCEDURES:

A. Initial Evaluation: Prior to executing a contract or delegation agreement with a potential FTE, 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 FTE to assume responsibility for delegated activities and to maintain IEHP standards, applicable Federal, State, 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 FTE 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 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) System for Award Management (SAM);
        3) The Medicare Opt-Out List;
        4) CMS Preclusion List ; and

5) The DHCS Medi-Cal Suspended and Ineligible Provider List (as applicable).

f. The entity's annual compliance and fraud, waste and abuse (FWA) training program.

2. An initial onsite evaluation may be conducted. If the FTE is not in full compliance with delegated standards, the FTE's action plan and timeline to achieve full compliance is reviewed. The oversight process may be modified for accredited/certified FTEs 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 FTE to verify compliance with established, revised, or new State, Federal, and accreditation requirements. The FTE is required to comply with IEHP reporting requirements.

3. Results and recommendations of the initial evaluation are documented in a report and presented to the Chief Operating Officer (COO). Copies of the results are reviewed by the Delegation Oversight Subcommittee and subsequently the Compliance Committee. To accommodate business needs, ad hoc meetings or electronic review and/or approval may substitute for routinely scheduled meetings.

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 FTE must submit data as contractually required.

D. Risk Areas: In identified risk areas, additional reporting may be required from the FTE. The FTE 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 FTE's ability to provide delegated services in accordance with contractual standards and applicable State, Federal, and accreditation requirements. High risk FTEs, 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 FTEs.

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 FTE 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 Disclosure documentation.
6. Exclusion of the FTE from participating in the federal health program (excluded parties lists):
    a. The DHHS OIG LEIE;
    b. The GSA SAM;
    c. The Medicare Opt-Out List ;
    d. CMS Preclusion List; and
    e. The DHCS Medi-Cal Suspended and Ineligible Provider List (as applicable).
7. Effective training and education that includes:
    a. General compliance.
    b. Code of Conduct distribution.
    c. Fraud, Waste and Abuse.
    d. HIPAA Privacy.
    e. Confidentiality Statement Attestations.
    f. Training Materials:
        1) Presentations.
        2) Sign-In Sheets/computer-based training completion reports.
        3) Certifications.

G. Focused Audits: If IEHP has a reason to believe the FTE'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, Federal, State, 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 FTE.

g. Significant changes in the management of the FTE.

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.

C. Annual Risk Assessment: An annual risk assessment will be completed to aid in identifying high risk FTEs. High risk FTEs 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. FTEs determined to be high risk may be subjected to a more frequent monitoring and auditing schedule.

1. The Delegation Oversight Committee will manage the annual comprehensive risk assessment process to determine the FTE'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 FTE deemed high risk or vulnerable is presented to the Compliance Committee for suggested action.

2. The Delegation Oversight Committee is tasked with oversight of the FTE Oversight process. The Committee reviews data and recommends modifications where appropriate. The key functions of the Delegation Oversight Committee for oversight of delegation management include:

   a. Monthly reviews of FTE performance data.

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

   c. Approval of the annual audit calendar and any ad-hoc monitoring and auditing.

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

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

   f. Provide reports at least annually to the IEHP Governing Board regarding monitoring and auditing activities conducted.

E. 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 FTE 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.

F. Training: IEHP will make training materials available to FTEs. However, it is expected that FTEs institute their own training program intended to communicate the compliance characteristics related to the FTE 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 FTEs. 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 Privacy.
2. 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 entities are also trained and have instituted a similar training program.

E. The functional areas and business departments implement the oversight 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 FTE relationship.
2. Identifying negative trends or vulnerabilities.
3. Monitoring FTE compliance according to the Program and associated tools and processes.
4. Monitoring operational performance.
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 FTE operational communications and/or training.
8. Reporting performance to the Delegation Oversight Committee.

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

INLAND EMPIRE HEALTH PLAN		
Regulatory/ Accreditation Agencies:	☐ DHCS	☐ CMS
	☐ DMHC	☐ NCQA
Original Effective Date:	January 1, 2014	
Revision Effective Date:	January 1, 2024	

23. COMPLIANCE

B. HIPAA Privacy and Security

APPLIES TO:

A. This policy applies to IEHP DualChoice (HMO D-SNP) Members, 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 compromise and/or liability to Members, entities and IEHP.
2. Entities must make reasonable efforts to safeguard the privacy and security of Members' Protected Health Information (PHI) and Personally Identifiable Information (PII); and are responsible for adhering to this policy and procedures, by using only the minimum necessary information 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, Standards for Privacy of Members' Identifiable Health Information, the administrative, physical, and technical safeguards of the HIPAA Security Rule, and any and all Federal regulations and interpretive guidelines promulgated there under.[1,2,3]
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.[4]
5. Entities must notify IEHP, their Members, the Centers for Medicare & 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.

DEFINITIONS:

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

[1] Title 45 Code of Federal Regulations (CFR) Part 160, 162, and 164
[2] Health Information Technology for Economic and Clinical Health Act (HITECH)
[3] American Recovery and Reinvestment Act of 2009
[4] 45 CFR §164.506(c)

to, a covered entity (IEHP). The types of functions or activities that may make a person or entity a business associate include treatment, payment, or health care operation 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.[5]

   1. PHI excludes individually identifiable health information in education records; in employment records held by a Covered Entity in its role as employer; and regarding a person who has been deceased for more than 50 years.[6,7]

   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. Medical information: Any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, reproductive or sexual health application information, mental or physical condition, or treatment.[8]

H. Sensitive services: All health care services related to mental or behavioral health, sexual and reproductive health, sexually transmitted infections, substance use disorder, gender affirming care, and intimate partner violence, and includes services described in Sections 6924, 6925, 6926, 6927, 6928, 6929, and 6930 of the Family Code, and Sections 121020 and 124260 of

[5] 45 CFR § 160.103
[6] Family Educational Rights and Privacy Act
[7] Title 20 United States Code § 1232(g)
[8] California Civil Code (Civ. Code) § 56.05(j)

the Health and Safety Code, obtained by a patient at or above the minimum age specified for consenting to the service.[9]

I. Breach: 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 PHI is presumed to be a breach unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised. Covered entities must consider a four (4) factor objective standard.[10]

1. The nature and extent of PHI involved (including the types of identifies and the likelihood of re-identification.);
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk of breach to the PHI has been mitigated.
5. Breach excludes:[11]
    a. Any unintentional acquisition, access, or use of PHI 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 PHI at a covered entity or business associate to another person authorized to access PHI 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 PHI 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. Due to unauthorized disclosures of PHI, confidentiality requirements were enhanced, which requires entities to be accountable for unauthorized access to medical information, not just for unlawful use or disclosure.[12]

[9] CA Civ. Code § 56.05(s)
[10] 45 CFR § 164.402
[11] Ibid.
[12] California Health and Safety Code (CA Health & Safety. Code) § 1280.15

1. Every entity must implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical record information and safeguard it from unauthorized access or unlawful access, use, or disclosure. Administrative fines for violations vary significantly.[13]
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 entities must educate their employees on privacy laws and their policy on privacy of medical information. The education should be documented and should include attendance.
4. Each entity is responsible for participating in ongoing education regarding Member privacy and Member rights.
5. Appropriate, documented action must be taken should an unauthorized access occur.

B. Only entities and their respective staff members with a legitimate business authorization may access, use or disclose Member information. This includes all activities related to treatment, payment and health care operations on behalf of IEHP. Each entity and their respective staff members may only access, use or disclose the minimum necessary information to perform his or her designated role regardless of the extent of access provided to him or her.[14]

C. With respect to entity system access, Member privacy must 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" found on the IEHP website).[15]

D. Each entity is responsible for ensuring staff members sign a Confidentiality Statement prior to access to PHI or PII and annually thereafter. Confidentiality statements must be retained for a period of six (6) years and include at minimum.[16]

   1. General Use;
   2. Security and Privacy Safeguards;
   3. Unacceptable Use; and

[13] 45 CFR § 164.530(c)
[14] 45 CFR § 164.502(b)
[15] https://www.iehp.org/en/providers/provider-resources?target=forms
[16] Department of Health Care Services (DHCS)-IEHP Two-Plan Contract, 1/10/20, Exhibit G, Attachment A, Section I. Personnel Controls, Paragraph C. Confidentiality Statement

4. Enforcement Policies.

E. Each entity is responsible for compliance in maintaining policies, principals and procedures related to the following:[17]

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 visitor 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 disposed of 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 entities' premises except for routine business purposes.

F. Permitted Uses and Disclosures[18]

1. 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.
2. PHI must be provided to patients, or their representative if requested, preferably in an electronic format, under HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH).
3. 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.
4. HIPAA gives the patient the right to make written requests to amend PHI that you are responsible for maintaining.
5. Upon patient request, an accounting of disclosures of PHI, and information related to such disclosures, must be provided to the patient.[19]

[17] 45 CFR §§ 160.202, 164.530(c)
[18] 45 CFR §§ 164.512
[19] 45 CFR § 164.528

G. Privacy Practices Notice

1. IEHP provides the "Notice of Privacy Practice" (See Attachment, "Notice of Privacy Practices" found on the IEHP website[20]) to each new Member as follows:[21]
   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.
   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.

H. Reporting of Unauthorized Access or Disclosures:[22]

1. IEHP or entities must only provide the following required notifications if the breach involved unsecured PHI. Unsecured PHI is PHI 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 PHI Affecting Fewer than 500 Individuals:[23]
   a. For breaches that affect fewer than 500 individuals, IEHP or entities 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 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 Breaches of Unsecured PHI Affecting 500 or more individuals:[24]
   a. If a breach affects 500 or more individuals, IEHP or entities must provide the Secretary of DHHS with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach. This 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 500 California residents as a result of a single breach of the security system, IEHP or entities shall electronically submit a single sample copy of that security breach

[20] https://www.iehp.org/en/providers/provider-resources?target=forms
[21] 45 CFR § 164.520
[22] 45 CFR§ 164.408
[23] 45 CFR § 164.408 (c)
[24] 45 CFR § 164.408 (b)

notification, excluding any personally identifiable information, to the Office of the Attorney General.[25]

c. In addition to notifying the affected Members, IEHP or entities 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 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:[26]

   a. If a breach notification form has been submitted to the Secretary and additional information is discovered, IEHP or entities 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):[27,28]

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

      1) By DHCS Privacy Incident Reporting Portal within 24 hours of discovery if PHI was or suspected to have been acquired by an unauthorized person.

      2) Within 10 calendar days of discovery of the breach a final, complete report 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 (HMO D-SNP) Members notify IEHP within 24 hours of discovery if PHI was, or suspected to have been, acquired by an unauthorized person. In the event that an entity provides notice to DHCS, IEHP should also be notified.

6. Member Breach Notifications:[29]

   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 Entities are required to also notify the affected Member(s) in written form and must be provided

[25] California Civil Code § 1798.29(e); California Civil Code §1798.82(f)
[26] United States Department of Health and Human Services (DHHS) of Public Law 111-5 § 13402(h)(2)
[27] 45 CFR §§ 164.400-414
[28] Department of Health Care Services (DHCS) -IEHP Two-Plan Contract, 1/10/20 (Final Rule A27), Exhibit G, Provision 3, Section J., Breaches and Security Incidents
[29] 45 CFR §§ 164.400-414

without unreasonable delay and in no case later than 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 Entities 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 Section

I. 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
By E-Mail to:	compliance@iehp.org
By Fax to:	(909) 477-8536

23. COMPLIANCE

B. HIPAA Privacy and Security

INLAND EMPIRE HEALTH PLAN		
Regulatory/ Accreditation Agencies:	☐ DHCS	☐ CMS
	☐ DMHC	☐ NCQA
Original Effective Date:	January 1, 2007	
Revision Effective Date:	January 1, 2024	

23. COMPLIANCE

C. Health Care Professional Advice to Members

APPLIES TO:

A. This policy applies to all IEHP DualChoice (HMO D-SNP) Members and Providers.

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 an IEHP Member whom they are caring for.[1]

PROCEDURE:

A. A health care professional shall be able to give advice or advocate for a Member regarding the Member's:[2]
   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 must inform Members of their 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. See Policies 9C, "Access to Care for People with Disabilities" and 9H1, "Cultural and Linguistic Services – Foreign Language Capabilities."

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.

[1] Title 42, Code of Federal Regulations (CFR) § 422.206
[2] Ibid.

23. COMPLIANCE

C. Health Care Professional Advice to Members

INLAND EMPIRE HEALTH PLAN		
Regulatory/ Accreditation Agencies:	☐ DHCS	☐ CMS
	☒ DMHC	☐ NCQA
Original Effective Date:	January 1, 2007	
Revision Effective Date:	January 1, 2024	