16. COMPLIANCE

A. HIPAA Privacy and Security

APPLIES TO:

A. This policy applies to all IEHP Covered 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, Providers, entities, and IEHP.
2. Entities must make reasonable efforts to safeguard the privacy and security of Members' Protected Health Information (PHI) and Personal Identifiable Information (PII); and are responsible for adhering to this policy 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, IEHP Covered, and the Secretary of 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 to, a covered entity (IEHP). The types of functions or activities that may make a person or

[1] Title 45 Code of Federal Regulations (CFR) §§ 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)

entity a business associate include treatment, 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.[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 (U.S.C) § 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]

~~G.~~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]
    1) 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.
    2) 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.
    3) 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] 45 CFR § 164.402
[12] California Health and Safety Code (CA Health & Safety Code) § 1280.15

16. COMPLIANCE

A. HIPAA Privacy and Security

1. Every healthcare 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 healthcare 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.

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

[13] 45 CFR § 164.530(c)
[14] 45 CFR § 164.502(b)
[15] https://www.iehp.org/en/providers/provider-resources?target=forms

E. Each entity is responsible for compliance in maintaining policies, principals and procedures related to the following:[16]

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:[17]

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.[18]

G. Privacy Practices Notice:

[16] 45 CFR §§ 160.202, 164.530(c)
[17] 45 CFR §§ 164.512
[18] 45 CFR § 164.528

1. IEHP provides the Notice of Privacy Practice. See "Attachment/Notice of Privacy Practices" found on the IEHP website, [19] to each new Member as follows:[20]
   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 Unauthorized Access or Disclosures:[21]

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:[22]
   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:[23]
   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

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

notification, excluding any personally identifiable information, to the Office of the Attorney General.[24]

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:[25]

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 IEHP Covered:

a. IEHP must notify IEHP Covered when a breach occurs that affects a IEHP Covered Member within the following timelines:

1) An initial report shall be made without reasonable delay, but no later than within three (3) business days to IEHP Covered.[26]

2) A final report will be filed withing three (3) calendar days of conducti8ng its investigation to IEHP Covered on the same form.[27]

3) IEHP follows the requirements in accordance with HIPAA Breach Notification Rule regarding privacy and security incident, (security incident defined in 45 C.F.R. § 164.304, reasonably calculated to result in a breach of personal identifiable information (PII) or PHI of IEHP Covered Members.[28]

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 without unreasonable delay and in no case later than 60 days following the discovery

[24] California Civil Code § 1798.29(e); California Civil Code § 1798.82(f)
[25] United States Department of Health and Human Services (DHHS) of Public Law 111-5 § 13402(h)(2)
[26] Covered California (CCA) Qualified Health Plan Issuer Contract, Article 10, Section 10.1(e), Breach Notification
[27] Ibid
[28] Ibid
[29] 45 CFR §§ 164.400-414

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 as follows:

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

16. COMPLIANCE

A. HIPAA Privacy and Security

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

16. COMPLIANCE

B. Health Care Professional Advice to Members

APPLIES TO:

A. This policy applies to all IEHP CoveredMembers 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 a Member regarding 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 C, "Access to Care for Members with Access and Functional Needs" and 4G1, "Cultural and Linguistic Services –Language Capabilities."

C. IEHP shall inform Members of their right to refuse treatment and information regarding advance directives in accordance with Policy 3D, "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.

16. COMPLIANCE

B. Health Care Professional Advice to Members

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