General Compliance Training
2017 Provider Manual

Compliance
Fraud, Waste and Abuse
HIPAA Privacy and Security

2017
Welcome to General Compliance Training for Providers!

**Training Objectives:**

- Understand why you need Compliance Training and how Compliance affects everyone
- Learn about the 7 Elements of an Effective Compliance Program
- Learn about Fraud, Waste and Abuse
- Learn about HIPAA/Privacy & Security
- Understand Reporting Requirements
**Mission Statement:** To organize and improve the delivery of quality, accessible and wellness based healthcare service for our community.
Compliance Training: Overview

Annual Compliance Training is mandatory for:
- Team Members
- Temporary Staff
- Contractors
- Providers
- Business Associates
- Vendors
- First tier, downstream and related entities (FDRs)
- Governing Board
- Chief Officers

Introductory Compliance Training
- Within 90 days of hire, all new Team Members & Temporary Staff, and contractors must attend Introductory Compliance Training
- Newly assigned Governing Board Members will be provided Compliance Training upon assignment to the Board

All First Tier Entities, including IPAs, must provide Compliance training to their staff and attest on an annual basis to IEHP that they have provided training to their employees and FDRs.
What is Compliance and Why is it Important?

Federal and State laws regulate the Health Care Industry

- To ensure compliance with applicable laws
- To protect our Members
- To prevent abuse of federal and state tax payer money
- To guide IEHP/FDRs to always do the right thing!
Everyone has a Role in Compliance

- Team Members
  - Temporary Staff
  - Interns
- Business Associates
  - Vendors
  - Contractors
- First Tier Entity
  (e.g., IPA, Hospital, Pharmacy Benefit Manager (PBM), etc.)
- Downstream Entity
  (e.g., Pharmacy contracted with PBM, claims processing contracted with IPA)
- Related Entity
  (e.g., common ownership or control of entity)

This group is also known as “FDRs”
Corporate Compliance Program Structure
OIG Guidance: 7 Elements

The Federal Sentencing Guidelines (FSG) and Office of Inspector General (OIG) have identified 7 Elements of an Effective Compliance Program:

- Governance / Board Oversight
- Compliance Professional
- Code of Conduct and Policies & Procedures
  - Employee Training
  - Reporting & Communication
  - Monitoring & Auditing
- Corrective Action
Written Policies, Procedures and Standards of Conduct
Written Policies, Procedures and Standards of Conduct

All Team Members and FDRs are expected to be familiar with IEHP policies and procedures, including the following:

- Show commitment to comply with both Federal and State standards
- Provide guidance to Team Members, Business Associates, Vendors and FDRs with issues related to Fraud, Waste and Abuse, HIPAA Privacy & Security, and other issues of non-compliance.
- Identify how to communicate compliance issues
- Describe how potential compliance issues are investigated
IEHP Code of Business Conduct and Ethics

Provides guidance to Team Members, Governing Board, Temporary Employees and Contractors about our Culture of Compliance and our role in preserving this culture.

Provides the requirements for FDRs to fully participate in any investigation, as needed.

Guides you in your responsibility to report incidents of non-compliance without fear of intimidation and/or retaliation.

IEHP also provides a Vendor Code of Conduct that mirrors our internal standards for our Business Associates, IPA’s, Hospitals and other FDRs.
Compliance Officer, Compliance Committee and High Level Oversight
Role of the Compliance Officer

The Compliance Officer is responsible for the oversight of IEHP’s:
- Oversight of FDRs
- Compliance Program
- Compliance Committee

The Compliance Officer is responsible to:
- IEHP’s Chief Executive Officer (CEO)
- IEHP’s Governing Board

The Compliance Officer is responsible for reporting on a quarterly basis to the Governing Board regarding all Compliance issues, including, but not limited to:
- Fraud, Waste and Abuse
- Privacy
- Auditing and Monitoring
- Non-compliant activities
Organizational Structure of IEHP Committees

JPA Board
- Chief Executive Officer
- Provider Advisory Council
  - Chief Medical Officer
    - Quality Management Committee
      - Compliance Committee
      - Policies and Procedures Subcommittee
      - Delegation Oversight Subcommittee
      - Auditing & Monitoring Subcommittee
      - Fraud, Waste and Abuse Subcommittee
      - Peer Review Subcommittee
      - Utilization Management Subcommittee
      - Pharmacy & Therapeutics Subcommittee
      - Credentialing Improvement Subcommittee
      - Persons with Disabilities Workgroup
      - Coordinated Care Initiative Stakeholder Advisory Committee
  - Chief Marketing Officer
    - Public Policy Participation Committee
Effective Training and Education
Compliance Training: A CMS Requirement

The following is from Chapter 21 of the Medicare Managed Care Manual

The sponsor must establish, implement and provide effective training and education for its employees, including the CEO, senior administrators or managers, and for the governing body members, and FDRs.

Effectiveness of training, education, compliance policies and procedures, and Standards of Conduct will be apparent through sponsor’s compliance with all Medicare program requirements. Sponsors must ensure that employees are aware of the Medicare requirements related to their job function.

The training and education must occur at least annually and be made a part of the orientation for new employees, including the chief executive and senior administrators or managers, governing body members, and FDRs.

Sponsors must be able to demonstrate that their employees have fulfilled these training requirements. Examples of proof of training may include copies of sign-in sheets, employee attestations and electronic certifications from the employees taking and completing the training.
Effective Lines of Communication
The sponsor must establish and implement effective lines of communication, ensuring confidentiality between the compliance officer, members of the compliance committee, the sponsor’s employees, managers and governing body, and the sponsor’s FDRs. Such lines of communication must be accessible to all and allow compliance issues to be reported including a method for anonymous and confidential good faith reporting of potential compliance issues as they are identified.
Element 5

Well-Publicized Disciplinary Standards
Disciplinary Standards: Consequences of Non-Compliance

FDRs are required to review the Department of Health and Human Services OIG List of Excluded Individuals and Entities and the General Services Administration System for Award Management prior to the hiring or contracting of any new employee, temporary employee, volunteer, consultant, governing body member, or FDR, and monthly thereafter to ensure that none of these persons or entities are excluded or become excluded from participation in federal programs.

First tier or downstream entity found to be non-compliant, are subject to disciplinary actions, up to and including contract termination.

No Federal health care program payment may be made for any item or service furnished, ordered, or prescribed by an individual or entity excluded by the OIG.
Effective Systems for Routine Monitoring, Auditing and Identification of Compliance Risks
Why spend time evaluating?

- To help ensure compliance with State and Federal laws and regulations
- Reduce risk for government programs against non-compliance and FWA
- Help correct any non-compliance with a corrective action plan that includes ongoing monitoring and auditing

Monitoring

Internal monitoring activities are regular reviews that confirm ongoing compliance and ensure that corrective actions are undertaken and effective.

Auditing

Internal auditing is a formal review of compliance with a particular set of standards procedures that are used as a base measure.
Procedures and Systems for Prompt Response to Compliance Issues
What happens when a potential issue is reported to Compliance?

Compliance reviews report of non-compliance and determines if an investigation is needed. Appropriate actions are taken based upon the report.

Compliance may require a corrective action plan (CAP).

The Compliance Officer provides monthly reports of compliance activities to Chief Officers, and as necessary, Directors.

Quarterly reports of compliance activities are provided at the Compliance Committee.

Quarterly reports of compliance activities are provided to the Governing Board.
Fraud, Waste and Abuse Program

Fraud, Waste and Abuse

• Detection, Correction and Prevention
**Fraud, Waste and Abuse Program**

### What is Fraud?

<table>
<thead>
<tr>
<th>Fraud</th>
<th>Some examples are:</th>
</tr>
</thead>
</table>
| The **intentional** (knowing and willful intent) misrepresentation of data or facts for financial gain. It occurs when a person knows or should know that something is false and knowingly deceives someone for monetary gain. | • Billing for services not furnished or provided  
• Soliciting, offering, or receiving a kickback, bribe or rebate  
• Offering beneficiaries a cash payment or other incentive to enroll in the plan  
• Intentionally and repeatedly billing at a higher rate, or unbundling claims  
• Collecting higher co-pays than specified  
• Using someone else’s Member ID to receive services  
• Medical identity theft (using someone else’s ID card)  
• Eligibility (Member stating they live in a service area; misstatement of income)  
• Drug seeking behavior (Doctor Shopping; Selling Medication)  
• Billing for prescriptions that are never picked up  
• Additional dispensing fees for split prescriptions when entire prescription cannot be filled |
Waste

- The **overutilization of services** that result in unnecessary costs. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources. It is the extravagant, careless or needless expenditure of healthcare benefits and/or services, which results in unnecessary costs. Waste is considered a misuse of resources.

<table>
<thead>
<tr>
<th>Waste</th>
<th>Some examples are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Providing medically unnecessary services, such as additional tests or procedures; and</td>
<td></td>
</tr>
<tr>
<td>• Failure to provide medically necessary services</td>
<td></td>
</tr>
<tr>
<td>• Performing unnecessary services for the member</td>
<td></td>
</tr>
</tbody>
</table>
## What is Abuse?

**Abuse**

- Includes actions that may, directly or indirectly, result in: unnecessary costs, improper payment, payment for services that fail to meet professionally recognized standards of care, or services that are medically unnecessary.
- Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

**Some examples are:**

- Re-ordering the same lab tests because the report could not be found in the chart
- Providing services that do not meet professionally recognized standards
- Inadvertently and consistently using the incorrect billing code on a claim
- Failure to effect timely disenrollment of a beneficiary from CMS systems
- Hospital billing issues, e.g. incorrect billing practices
- Overprescribing narcotics
Federal Healthcare Fraud Laws

**False Claims Act (FCA)**
- **California**
  - Recovered hundreds of millions of dollars
  - Liable for up to three times the amount of money fraudulently obtained
  - Whistleblower protection
- **Federal**
  - Imposes liability on individuals or entities who defraud governmental programs
  - Whistleblower protection
  - 2014: 89% of all False Claim actions were initiated by whistleblowers
  - 2014: 5.7 billion dollars recovered

**Anti-Kickback Statute**
- Knowingly or willfully soliciting, receiving, offering or paying for referrals for services (e.g. kickback, bribe, or rebate)
- Violations are punishable by a fine of up to $25,000; imprisonment for up to 5 years; or both.

**Stark Statute Damages and Penalties**
- Prohibits a physician from referring Medicare patients for designated health services to an entity with which the physician (or a member of his or her family) has a financial relationship, unless an exception applies
- Prohibits the designated health services entity from submitting claims to Medicare for those services resulting from a prohibited referral
- A penalty of up to $15,000 may be imposed for each service provided; may also be up to a $100,000 fine for entering into an unlawful arrangement.

**Civil Monetary Penalty:**
Penalty range from $5,500 and $11,000 for each false claim and damages may be tripled.
Repercussions of Committing Fraud, Waste, or Abuse

Potential penalties, depending on the violation

- Civil Monetary Penalties
- Criminal Conviction/Fines
- Civil Prosecution
- Imprisonment
- Loss of Provider License
- Exclusion from Federal Health Care programs
• Every Team Member has the right and responsibility to report suspected Fraud, Waste and Abuse.

• Not reporting fraud or suspected fraud can make you a party to a case by allowing the fraud to continue.

• You may report anonymously and retaliation is prohibited when you report a concern in good faith.
HIPAA/Privacy & Security

Health Insurance Portability and Accountability Act

Privacy and Security
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Creates greater access to health care insurance, protection of privacy of health care data, and promotes standardization and efficiency in the health care industry.
- Provides safeguards to prevent unauthorized access to protected health care information.
- As an FDR who has access to protected health care information of our members, you are responsible for complying with the HIPAA guidelines.
- Violations may result in civil monetary penalties. In some cases, criminal penalties may apply.
HIPAA

Requires that healthcare entities take specific steps to ensure that Member protected health care information (PHI) is not viewed by anyone without “a business need to know,” is not stolen, lost or accidentally destroyed.

Requires that Members be provided with rights over the use and disclosure of their own PHI.

HIPAA Security Rule covers information that is stored or transmitted electronically.

HIPAA Privacy Rule covers certain health information in any form.
### Definitions & Key Terms

**Protected Health Information (PHI)**
- Individually identifiable health information that relates to a Member’s past, present or future physical or mental health or condition, including the provision of his/her health care, or payment for that care (such as claims, enrollment and disenrollment).
- A breach of PHI means the impermissible access, use or disclosure of PHI which compromises the security or privacy of the PHI.

**Personally Identifiable Information (PII)**
- Information that either identifies the Member or there is a reasonable basis to believe that the information can be used to identify the Member, such as name, date of birth, address, or Social Security Number. Other personal identifiers include, but are not limited to, IEHP identification number, phone numbers, e-mail addresses, photographic images, financial information, such as transaction receipts, bank account or credit card numbers.

**Minimum Necessary**
- All reasonable efforts should be made to access, use, disclose and request only the minimum amount of PHI needed to accomplish the intended purpose of the access, use, disclosure or request.
Common PHI Breaches

– Unauthorized access
  • Family/Friends Accounts
  • Viewing Member information without a “business need to know” (ask “Do I need to access this information to do my job?”)

– Misdirected documents
  • Sending documents to an incorrect fax number
  • Mailing / handing documents by mistake to the wrong Member

– Unauthorized verbal disclosure
  • phone
  • voicemail
  • in person

– Lost, missing or stolen mobile devices that contain unencrypted data
  • Phones, laptops, tablets

– Improper disposal of documentation, computers or other materials (e.g. throwing in regular trash)

– Unsecured E-Mail containing Member information

– Web access creating data security risks (social media)
Treatment, Payment and Operations

The law only allows disclosure of PHI under the following categories:

(T) Treatment
When the information requested is needed to treat our Member

(P) Payment
When the information is needed to provide payment for services that a Member received

(O) Operations
When the information is used for health care operations

Questions?
Ask Us!

Do I need to know this information to do my job?
### Privacy Training Tips

1. **Never discuss PHI where you may be overheard**
2. **Access Member PHI only when it pertains to your job tasks**
3. **Use shredder bins to destroy PHI**
4. **Confirm phone number and fax numbers prior to use**
5. **Confirm you are speaking with the Member or authorized representative before discussing PHI**
6. **Lock your computer when leaving your work area**
Privacy Training Tips for the General Medical Setting

Every staff member in the office should be apprised of HIPAA standards and held accountable.

Do not discuss sensitive issues when the patient is standing in the reception window and within earshot of those in the waiting room.

Use a patient sign-in system that allows the reception staff to remove or obstruct the name after sign-in.

When retrieving a patient from the waiting room for their appointment, use only the first name.

When placing charts for the physician, position in such a way that patient names are not visible.

Offices should have a partition system/window so that those in the waiting area cannot hear business conducted by staff members.

When leaving appointment reminder phone calls to patient, exercise caution not to leave PHI in your message.
Security Training Tips

- Assure that office staff use a secure method for sending E-Mail containing PHI
- Assure that the office server is in a secure area
- Paper based PHI should always be kept in a secure area
- Change passwords often
- Do not leave passwords/log-on info in office area (on monitor, under keyboard)
- Password sharing is prohibited by policy - **Do not share your password with anyone**
- Use an auto log-off or screen saver
- When leaving work area, lock your workstation
Now that you know how to identify issues of noncompliance, it’s your responsibility to report suspected or actual compliance concerns.
Ways to Report Compliance Concerns

Reporting suspected or detected non-compliance, FWA or Privacy Issues is your responsibility.

- **Hotline:** 866-355-9038
- **E-Mail:** compliance@iehp.org
- **Fax:** (909) 477-8536
- **Mail:**
  IEHP Compliance Officer
  P.O. Box 1800
  Rancho Cucamonga, CA 91729
How does someone outside of IEHP know how to report?

Information is published in the Member Handbook, the Provider Manual, on the IEHP Website and in the Vendor Code of Conduct.
Reporting Compliance Issues (cont.)

Reporting issues of Non-Compliance
- To the extent that the law allows, reports are confidential
- FDRs are required to participate in any investigation, as necessary
- Reports can also be anonymous

What kind of behavior/incidents are reportable?
- Behavior that is against the Code of Business Conduct and Ethics;
- Suspected Fraud, Waste and Abuse
- Suspected Privacy Issues

What can happen if you fail to report an incident that they you are aware of?
- May be subject to disciplinary actions, up to and including termination

IEHP has a non-retaliation policy
- Individuals who retaliate with discriminatory behavior or harassment against an individual who has reported an issue will be subject to disciplinary actions, up to and including termination
IEHP’s Compliance Department is your resource for questions or concerns related to compliance, FWA and Privacy issues. We are here to help you do the right thing.

- **Hotline:** 866-355-9038
- **E-Mail:** compliance@iehp.org
- **Fax:** (909) 477-8536
Thank you for participating and expanding compliance program effectiveness by ensuring you and your organization incorporate the information into your individual compliance program and business practices.