2019-2020 Provider Manual Compliance Training

Compliance
Fraud, Waste and Abuse (FWA)
HIPAA Privacy and Security

Presented by: IEHP Compliance Department

Agenda

Welcome to Compliance Training for Providers and IPAs!

- Compliance Program
  - Seven Elements of an Effective Compliance Program
- Ethics: Doing the Right Thing
- Issues of Non-Compliance
- Fraud, Waste and Abuse (FWA)
- HIPAA Privacy & Security
- Reporting Requirements

Training Objectives

- Understand why you need Compliance Training and how Compliance affects everyone

- Recognize How a Compliance Program Operates

- Learn About Fraud, Waste and Abuse (FWA)

- Learn About HIPAA Privacy & Security

- Know How To Report Issues & Understand Reporting Requirements

Where do I fit in?

- As a person providing health care or administrative services to Medi-Cal/Medicare enrollees, you are likely an employee of a Provider or subcontracted delegated entity.
- IEHP enters into contracts with subcontracted delegated entities to fulfill contractual obligations.

Why Do I Need Training?

- Compliance is everyone's responsibility!
  As an individual who provides health care or administrative services to Medi-Cal and Medicare enrollees, every action you take potentially affects these enrollees; Medi-Cal and Medicare Programs.
- Every year, billions of dollars are improperly spent because of Fraud, Waste and Abuse (FWA). It affects everyone—including *you*. This training helps you detect, correct, and prevent FWA. ***You are part of the solution***.

Compliance Program Requirements

- IEHP Regulators require that we implement and maintain an effective compliance program. IEHP requires the same of our delegated entities, including IPAs. An effective compliance program must:
  - Articulate and demonstrate an organization's commitment to legal and ethical conduct.
  - Provide guidance on how to handle compliance questions and concerns.
  - Provide guidance on how to identify and report compliance violations.

What is an Effective Compliance Program?

- An effective compliance program fosters a culture of compliance within an organization, at a minimum:
  - Prevents, detects, and corrects non-compliance
  - Is fully implemented and is tailored to an organization's unique operations and circumstances
  - Has adequate resources
  - Promotes the organization's Standards of Conduct
  - Establishes clear lines of communication for reporting non-compliance
- An effective compliance program is essential to prevent, detect, and correct non-compliance, as well as, Fraud, Waste and Abuse (FWA). It must, at a minimum, include the Seven Core Elements of an Effective Compliance Program.

For more information see the Office of Inspector General (OIG) website: https://oig.hhs.gov/compliance/compliance-resource-portal/files/HCCA-OIG-Resource-Guide.pdf

Compliance Program

Seven Elements of an Effective Compliance Program:

1. Written Policies, Procedures, and Standards of Conduct
   - These articulate the commitment to comply with applicable Federal and State standards and describe compliance expectations according to the Standards of Conduct.

2. Compliance Officer, Compliance Committee and High-Level Oversight
   - There must be a designated Compliance Officer and a Compliance Committee; who are accountable and responsible for the activities and status of the Compliance Program, including: issues identified, investigated, and resolved by the Compliance Program.
   - Senior Management and Governing Body must be engaged and exercise reasonable oversight over the Compliance Program.

3. Effective Training and Education
   - This covers the elements of the Compliance Plan as well as preventing, detecting and reporting FWA. The training and education are to be tailored for the different employees and their roles and responsibilities.

Seven Elements of an Effective Compliance Program (cont'd):

4. Effective Lines of Communication
   - Make effective lines of communication accessible to all, ensure confidentiality, and provide methods for anonymous and good-faith compliance issues reporting.
5. Well-Publicized Disciplinary Standards
   - Enforce standards through well-publicized disciplinary guidelines.
6. Effective System for Routine Monitoring, Auditing, and Identifying Compliance Risks
   - Conduct routine monitoring and auditing of operations to evaluate compliance with requirements, as well as the overall effectiveness of the Compliance Program
7. Procedures and System for Prompt Response to Compliance Issues
   - Use effective measures to respond promptly to non-compliance and undertake appropriate corrective action.

Operating an Effective Compliance Program
- Create a proactive Compliance Program
- Develop processes to evaluate and measure Compliance Program Effectiveness:
    - Develop benchmarks and goals in the team with the Compliance Committee, Board, and department leadership
    - Determine metrics – what do you want to measure?
    - Train your staff and test knowledge
    - Encourage Compliance Staff education and networking internally and externally
    - Solicit feedback
    - Maintain visibility
    - Enforce Policies and Procedures
    - Act promptly when issues arise
    - Take and document corrective action

Ethics: Do the Right Thing!

As a Provider and/or delegated entity of IEHP, you must conduct yourself in an ethical and legal manner. It's all about doing the right thing!

- Act fairly and honestly
- Adhere to high ethical standards in all you do
- Comply with all applicable laws, regulations, and regulatory agency requirements
- Report suspected violations

IEHP requires delegated entities to develop and implement a Code of Conduct or to adopt IEHP's Code of Business Conduct and Ethics, which can be found on IEHP.org.

The Code of Conduct states IEHP's compliance expectations and our operational principles and values. Reporting Code of Conduct violations and suspected non-compliance is everyone's responsibility.

Non-Compliance

What is Non-Compliance?

- Non-compliance is conduct that does not conform to the law, State, or Federal health care program requirements, or the ethical and business policies.

Know the Consequences of Non-Compliance

- Failure to follow the requirements can lead to serious consequences including:
    - Financial Sanctions
    - Contract Termination
    - Criminal Penalties
    - Exclusion from participating in all State and/or Federal health care programs
- Additionally, disciplinary standards for non-compliant behavior are required.

Non-Compliance Affects Everybody

- Without programs to prevent, detect, and correct non-compliance, we all risk:
  - Harm to Patients/Members, such as delayed services, denial of benefits, difficulty in using Providers of choice and other hurdles to care
  - Loss of contracts or licensures

Fraud, Waste and Abuse (FWA) Training

Inland Empire Health Plan
A Public Entity

Training Objectives

- Recognize FWA

- Learn about the FWA laws and regulations

- Recognize potential consequences and penalties associated with violations

- Understand your role for identifying and reporting FWA issues

Defining FWA

- *Fraud* is knowingly and willfully executing or attempting to execute, a scheme or artifice to defraud a health care benefit program, or to obtain, by means of fraudulent pretenses, representations, or promises, any of the money of property owned by, or under the custody or control of, any health care benefit program.
- *Waste* includes overusing services, or other practices that, directly or indirectly result in unnecessary health care costs. Waste is generally not considered to be caused by criminally negligent actions but rather by the misuse of resources.
- *Abuse* includes actions that may, directly or indirectly, result in unnecessary health care costs. Abuse involves payment for items or services when there is not a legal entitlement to that payment and the Provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

One of the primary differences between these is intent and knowledge.

Examples of FWA

- Actions that may constitute *Fraud* include:
  - Knowingly billing for services not furnished or supplies not provided
  - Billing for nonexistent prescriptions
  - Knowingly altering claims forms, medical records, or receipts to receive a higher payment
- Actions that may constitute *Waste* include:
  - Conducting excessive office visits or writing excessive prescriptions
  - Prescribing more medications than necessary for treating a specific condition
  - Ordering excessive laboratory tests
- Actions that may constitute *Abuse* include:
  - Unknowingly billing for unnecessary medical services
  - Unknowingly billing for brand name drugs when generics are dispensed
  - Unknowingly excessively charging for services or supplies
  - Unknowingly misusing codes on a claim, such as upcoding or unbundling codes

Understanding FWA

To detect FWA, you need to know the laws & regulations:

- Civil False Claims Act, Health Care Fraud Statute, and Criminal Fraud
- Anti-Kickback Statute
- Stark Statute (Physician Self-Referral Law)
- Exclusion from all Federal and State health care programs

Civil False Claims Act (FCA)

- Civil provisions of the FCA make a person liable to pay damages to the Government if he/she knowingly:
  - Conspires to violate FCA
  - Carries out other acts to obtain property from the Government by misrepresentation
  - Conceals or improperly avoids or decreases an obligation to pay the Government
  - Makes or uses a false record or statement supporting the false claim
  - Presents a false claim for payment or approval

  Example:
  - The owner-operator of a medical clinic in California used marketers to recruit individuals for medically unnecessary office visits. They also promised free, medically unnecessary equipment or free food to entice individuals. They charged Medicare more than $1.7 million for the scheme. They were sentenced to 37 months in prison.

Civil False Claims Act (FCA) continued

Any person who knowingly submits false claims to the Government is liable for three times the Government's damages caused by the violator plus a penalty.

- *Whistleblowers-* Person who exposes information or activity that is deemed illegal, dishonest, or violates professional or clinical standards.
- *Protected-* Persons who report false claims or bring legal actions to recover money paid on false claims are protected from retaliation.
- *Rewarded-* Persons who bring a successful whistleblower lawsuit receive at least 15%, but not more than 30%, of the money recovered.

For more information, refer to 31 United States Code (USC) Sections 3729-3733

Health Care Fraud Statute

- States "Whoever knowingly and willfully executes, or attempts to execute a scheme or artifice to defraud any health care benefit program…shall be fined under this title or imprisonment not more than 10 years , or both."
- Conviction under the statute does not require proof the violator had knowledge of the law or specific intent to violate the law.

Example:

- A Pennsylvania pharmacist submitted claims to a Medicare Part D plan for non-existent prescriptions and drugs not dispensed. They pled guilty to health care fraud and received a 15-month prison sentence and was ordered to pay more than $166,000 in restitution to the Health Plan.

For more information, refer to 18 USC 1346-1347.

Criminal Health Care Fraud

- Persons who knowingly make a false claim may be subject to:
    - Criminal fines up to $250,000
    - Imprisonment up to 20 years
- If the violations resulted in death, the individual may be imprisoned for any term of years or for life.

For more information, refer to 18 USC 1347.

Anti-Kickback Statute

- Prohibits knowingly and willfully soliciting, receiving, offering, or paying remuneration (including any kickback, bribe, or rebate) for referrals or services that are paid, in whole or in part under Federal health care program.
- Violations are punishable by:
  - A fine of up to $250,000
  - Imprisonment up to 5 years

  Example:
  - From 2012 through 2015, a physician operating a pain management practice in Rhode Island conspired to solicit and receive kickbacks for prescribing a highly addictive version of the opioid Fentanyl. They reported that patients had breakthrough cancer pain to secure insurance payments. They received $188,000 in speaker fee kickbacks from the drug manufacturer. The kickback scheme cost Medicare and other payers more than $750,000. The physician must pay more than $750,000 restitution and is awaiting sentencing.

For more information, refer to 42 USC 1320a-7b(b).

Stark Statute (Physician Self-Referral Law)

- Prohibits a physician from making referrals for certain designated health services to an entity when the physician (or a Member of his or her family) has:
  - An ownership/investment interest
  - A compensation agreement
- Claims tainted by an arrangement that does not comply with the Stark Statute are not payable. A penalty of around $24,250 can be imposed for each service provided. There may also be a fine of around $161,000 for entering into an unlawful arrangement or scheme
  - For more information, visit the Physician Self-referral web page and refer to the Act, Section 1877.

  Example:
  - A California hospital was ordered to pay more than $3.2 million to settle Stark Law violations for maintaining 97 financial relationships with physicians and physician groups outside the fair market value standards of that were improperly documented as exceptions.

Exceptions may apply. For more information refer to 42 USC Section 1395nn.

Civil Monetary Penalties Law

- The Office of Inspector General (OIG) may impose civil penalties for several reasons, including:
  - Arranging for services or items from an excluded individual or entity
  - Providing services or items while excluded
  - Failing to grant OIG timely access to reports
  - Knowing of and failing to report and return an overpayment
  - Making false claims
  - Paying influence referrals
- The penalties can be around $15,000 to $70,000 depending on specific violation. Violators are also subject to three times the amount:
  - Claimed for each service or item or
  - Of remuneration offered, paid, solicited or received

  Example:
  - A California pharmacy and its owner agreed to pay $1.3 million to settle allegations that they submitted unsubstantiated claims to Medicare Part D for brand name prescription drugs the pharmacy could not have dispensed based on inventory records.

For more information, refer to 42 USC 12320a-7a and the Act, Section 1128A(a)

Exclusion

- 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. The OIG has authority to exclude individuals and entities from federally funded health care programs and maintains the List of Excluded Individuals and Entities (LEIE)
- The U.S. General Services Administration (GSA) administers the Excluded Parties List System (EPLS), which contains debarment actions taken by various Federal agencies, including the OIG. Access to the EPLS is available through the System for Award Management (SAM) website.
- Medi-Cal maintains the Suspended and Ineligible (S&I) Provider List of health care Providers and entities that have been barred from participation in the Medi-Cal program.
- When looking for excluded individuals or entities, check all the LEIE, EPLS and the S&I lists, since they may not be the same.

Example:
  - A pharmaceutical company pled guilty to two felony counts of criminal fraud related to failure to file required reports with the U.S. FDA concerning oversized morphine sulfate tablets. The pharmaceutical firm executive was excluded based upon the company's guilty plea.

Exclusion, Continued

IEHP does not contract or employ anyone excluded from participation in Federal and/or State health care programs.

Per Provider Manual policies, Medicare DualChoice MA_24E and Medi-Cal MA_24E, Delegated entities must implement a screening program for employees, Board Members, contractors, and business partners to avoid relationships with individuals and/or entities that tend toward inappropriate conduct.

For more information refer to 42 USC Section 1320a-7 and 42 Code of Federal Regulations (CFR) Section 1001.1901

Your Role in Preventing, Detecting & Reporting Potential FWA

Take Action against FWA by following 3 steps:

- First, you must _comply_ with all applicable statutory and regulatory requirements, including adopting and using an effective compliance program.
- Second, you have a duty to _report_ any compliance concerns and suspected or actual violations of which you may be aware.
- Third, you have a duty to _conduct_ yourself in a manner that aligns with the Code of Conduct which articulates a commitment to standards of conduct and ethical rules of behavior.

Prevent FWA:

- Look for suspicious activity
- Conduct yourself in an ethical manner
- Ensure accurate and timely data and billing
- Ensure coordination with other payers
- Know FWA policies and procedures, standards of conduct, laws, regulations and CMS' guidance
- Verify all received information

Report FWA

- Everyone must report potential or suspected instances of FWA. The Code of Conduct should clearly state this obligation. There should also be a zero retaliation clause for good faith reporting of these instances.
- A mechanism for reporting should be readily available for employees and FDRs with the capability for the reporter to remain anonymous.
- Potential FWA instances should be reported to the appropriate regulatory entity, as well as IEHP.

Correct FWA

- Once FWA is detected, promptly correct it. Correcting the problem saves money and ensures compliance with regulatory requirements.
- Develop a plan to correct the issue. Ask your organization's Compliance Officer about the development process for the corrective action plan. A general action plan should:
  - Design the corrective action to correct the underlying problem that results in FWA program violations and to prevent future non-compliance.
  - Tailor corrective action to address particular FWA, problem, or deficiency identified. Include timeframes for specific actions.
  - Document corrective actions addressing non-compliance or FWA committed by the employee and include consequences for failure to satisfactorily complete the corrective action.
  - Monitor corrective actions continuously to ensure effectiveness.

Indicators of Potential FWA

- Now that you know about your role in preventing, reporting, and correcting FWA, let's review some key indicators to help you recognize the signs of someone committing FWA.
- Here are some questions to ask yourself in the different areas, depending on your role.
  - Key Indicators: Potential Member/Patient Issues
    - Does the prescription, medical record, or laboratory test look altered or possibly forged?
    - Does the Member's/Patient's medical history support the services requested?
    - Have you filled numerous identical prescriptions for this Member/Patient, possibly from different doctors?
    - Is the person receiving the medical service the Member/Patient (identity theft)?
    - Is the prescription appropriate based on the Member's/Patient's other prescriptions?

Indicators of Potential FWA, continued

- Key Indicators: Potential Provider Issues
  - Are the Provider's prescriptions appropriate for the Member's/Patient's health condition (medically necessary)?
  - Does the Provider bill the Plan for services not provided?
  - Does the Provider write prescriptions for diverse drugs or primarily for controlled substances?
  - Is the Provider performing medically unnecessary services for the Member/Patient?
  - Is the Provider prescribing a higher quantity than medically necessary for the condition?
  - Does the Provider's prescription have their active and valid National Provider Identifier on it?
  - Is the Provider's diagnosis for the Member/Patient supported in the medical record?

Indicators of Potential FWA continued

- Key Indicators: Potential Pharmacy Issues
  - Are drugs being diverted (drugs meant for nursing homes, hospice, and other entities being sent elsewhere)?
  - Are the dispensed drugs expired, fake, diluted, or illegal?
  - Are generic drugs provided when the prescription requires dispensing brand drugs?
  - Are Health Plans billed for unfilled or prescriptions not picked up?
  - Are proper provisions made if the entire prescription is not filled (no additional dispensing fees for split prescriptions)?
  - Do you see prescriptions being altered (changing quantities or Dispense As Written)?

HIPAA Privacy & Security Training

Inland Empire Health Plan

Training Objectives

- Review HIPAA Privacy and Security

- Review key terms and definitions

- Understand when it's appropriate to access Member/Patient information

- Explore your job function and what information you need to use to perform your tasks

Protecting Information

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 a Provider who has access to protected health care information of our Members/Patients, you are responsible for complying with the HIPAA guidelines.

Violations may result in civil monetary penalties. In some cases, criminal penalties may apply.

- Requires that health care 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/Patients 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.

Understanding PII and PHI

- *Personally Identifiable Information (PII)* is information that can either identify the Member/Patient or there is reasonable basis to believe that the information can be used to identify the Member/Patient.
  - For example- Name, Date of Birth, address, full Social Security number*, medical identification numbers, phone numbers, e-mail addresses, photographic images, driver's license number, etc.
    - *While a complete SSN can be used to identify an individual and is considered PII, the last 4 digits alone cannot be used to identify an individual, so it is not classified as PII.
- *Protected Health Information (PHI)* is health information that relates to a Member's/Patient's past, present or future physical or mental health or condition, including the provision of his/her health care, or payment for that care **AND** contains PII.

Privacy and Security Terms

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.

Access
- Ability to view, acquire or use Member/Patient PHI through authorized access to business systems, facilities or through any other means where PHI is available.

Authorization
- Must obtain Member's/Patient's written authorization for any use or disclosure of PHI that is not for treatment, payment, or operations or otherwise permitted or required by regulations and/or statutes.

Privacy Breach
- A privacy breach is defined as unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information.

Accessing PHI

Law allows access and disclosure of Member/Patient PHI when a request or need for information falls under Treatment, Payment or Operations (TPO).

(T) Treatment

PHI is used in the treatment of the Member/Patient.

Example- A nurse reviews a Member's/Patient's immunization record to assess which vaccines they will need at an upcoming visit.

(P) Payment

PHI is needed to provide payment for services a Member/Patient received.

Example – A request from IEHP to a Provider to obtain medical records in order to remit payment.

(O) Operations

PHI is needed to carry out health administration operations.

Example – A compliance investigator accessing authorizations for a Member/Patient when conducting a fraud investigation.

Appropriate vs. Inappropriate Access

Questions to ask yourself

- Do I have a business need or purpose to access this information?
- Do I need to access this information to do my job?
- Am I allowed through Treatment, Payment, or Operations (TPO) to use or disclose this information?
- Am I taking all necessary actions to safeguard PHI that I use?

Answers that may indicate inappropriate access

- It's easier to look this information up for my friend/family member rather than them having to call Member Services at IEHP.
- I've been asked to verify an address about one of our Members/Patients.
- This Member/Patient is my neighbor and I'm concerned about their care.
- My family member gave me permission to view their record.

Common PHI Breaches

- Unauthorized access
  - Family/Friends Accounts
  - Viewing Member information without a "business need to know"
- Misdirected documents
  - Sending documents to an incorrect fax number
  - Mailing / handing documents by mistake to the wrong Member/Patient
- Unauthorized verbal disclosure
  - In person – Use discretion near others who are in close proximity and may overhear
  - Phone
  - Voicemail
- Lost, missing or stolen mobile devices that contain unencrypted data (e.g. 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 (e.g., social media)

Protecting Information

Your responsibilities as a Provider:

- Never discuss PHI where you may be overheard
- Access Member/Patient PHI only when it pertains to your job tasks
- Securely destroy PHI
- Confirm phone number and fax numbers prior to use
- Pick up PHI from fax machines as they are received
- Confirm you are speaking with the Member/Patient or authorized representative before discussing PHI
- Treat Member/Patient PHI as you would expect your own PHI to be treated by others
- Secure/Lock PHI when leaving your work area and lock any other office equipment that man contain PHI/PII

Information Security

Health care organizations are particularly vulnerable to cyber attacks, since they house personal health, payment, and organizational proprietary information.

- Your Role?
  - Email Security – always think before you click
  - Be cautious when transmitting sensitive information – use secure mail procedures, if available, and verify recipient information prior to sending.
  - Report any information security issues related to IEHP Members to IEHP's Compliance Department.

Reporting Compliance

What to Report

- Conduct that does not conform to the law or State and Federal Health Care Programs.
- Unethical behavior that does not conform to your or IEHP's Code of Conduct
- Potential Fraud, Waste and Abuse (FWA)
- Potential Privacy issues/breaches

Reporting Facts

- Reports can be made anonymously
- To the extent that the law allows, reports are confidential
- Reporters are expected to participate in any investigation, as necessary
- Zero Tolerance of Intimidation/Retaliation for reporters

Reporting Options

- **IEHP's Compliance Toll Free Hotline:** 866-355-9038
- **E-Mail:** compliance@iehp.org
- **Webform:** www.iehp.org
- **Fax:** (909) 477-8536
- **Mail:**
  IEHP Compliance Officer
  Inland Empire Health Plan
  P.O. Box 1800
  Rancho Cucamonga, CA 91729

Notice

This training was prepared by the IEHP Compliance Department as a service to our Providers and delegated entities. The training may contain references, statutes, regulations or other policy materials. The information provided is only intended to be a general summary. It is not intended to take place of either the written law or regulations. We encourage you to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

Doing what's right, together.

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.

IEHP's Compliance Program is your resource for questions or concerns related to compliance, FWA, and Privacy & Security. We can be reached at compliance@iehp.org.

We are here to help you do the right thing!