IEHP
A Public Entity
Inland Empire Health Plan

2021-2022 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!

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

Compliance Training: Overview

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

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.

Compliance Program

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

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.

Compliance Program

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.

Compliance Program

Operating an Effective Compliance Program

- Create a proactive Compliance Program vs. reactive
- 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
- Act with integrity, transparency, and accountability
- Comply with all applicable laws, regulations, and regulatory agency requirements
- Report suspected violations

IEHP requires delegated entities to develop & 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-compliance behavior are required.

Examples of Non-Compliance

Examples of Non-Compliance	Explanation
"My co-worker changed a date on a member's authorization request to avoid getting in trouble for being late. I know this is wrong, but it only happened once, so I won't say anything."	Covering up unethical behavior is wrong. While you intended to protect your co-worker, you allowed harm to occur to the member.
"One patient needed a doctor's office visit on December 29th. He stated his insurance would not be effective until January 1st. My co-worker wanted to help the patient and changed the date of service in the medical record to January 2nd to ensure the patient's insurance covers the visit."	Knowingly entering inaccurate information in a record to ensure compensation is fraud and is a crime under the Federal False Claims Act. If you know or suspect fraud is occurring, you must report it immediately to management or compliance.

High Risk Areas for Non-Compliance

The following are examples of high-risk areas:

- Appeals and grievance review (for example, coverage and organization determinations)
- Beneficiary notices
- Conflicts of interest
- Claims and Utilization Management processing
- Credentialing and provider networks
- Documentation and Timeliness requirements
- IT System access and safeguards
- Ethics
- FDR oversight and monitoring
- Health Insurance Portability and Accountability Act (HIPAA)
- Marketing and enrollment
- Pharmacy, formulary, and benefit administration
- Quality of care
- Claims and Utilization Management documentation manipulation

Examples of Non-Compliance in High Risk Areas

Documentation and Timeliness Requirements

Examples of Non-Compliance	Explanation
"We received a request from a member to access their medical records. Our co-worker who handles these requests is out on medical leave for at least 2 more months. Due to our shortage of staff, can these types of requests wait until our co-worker returns?"	No. It is the law that medical records be provided within 30 days of the request
"The mailroom where we send out denial letters has been having issues. We have not told anyone, even though outgoing mail has been delayed for at least 2 days. This should not be an issue, right?"	This is an issue because denial letters have sensitive timelines. Delays in mailing should be reported immediately.

Examples of Non-Compliance in high Risk Areas

Claims Documentation Manipulation

Examples of Non-Compliance	Explanation
"Our patient wants a procedure not covered by his insurance as it is not considered medically necessary. A Physician Assistant knows the procedure would be covered by insurance for treatment of a specific diagnosis and adds this diagnosis to the insurance claim to ensure the procedure is covered."	Knowingly entering inaccurate information in a record to ensure compensation is fraud and is a crime under the Federal False Claims Act. If you know or suspect fraud is occurring, you must report it immediately to management or Compliance.

Examples of Non-Compliance in high Risk Areas

Conflict of Interests

Examples of Non-Compliance	Explanation
"A pharmaceutical representative has given our office tickets to a highly coveted sporting event in appreciation of all the business that we do with them. We know these are expensive and hard to come by – can we accept the tickets?"	No. This would be a conflict of interest and may create the perception that business is only conducted with those pharmaceutical companies that provide perks, and not those in the best interest of the member/enrollee

Reporting Non-Compliance

Reports of suspected non-compliance may be made anonymously and are kept confidential to the extent allowed by law.

A **whistleblower** is a person who exposes information or activity that is deemed illegal, dishonest, or violates professional or clinical standards.

Whistleblowers and persons who report in good-faith any suspected violations or issues, are protected from retaliation and intimidation.

Examples of Non-Compliance	Explanation
"After I reported irregularities in my department, my manager began excluding me from meetings and moved me to an undesirable location in the office."	Retaliation or intimidation is not tolerated. The manager's behavior is unacceptable and should be reported to management or to Compliance.

Anonymity vs. Confidentiality

- Remaining **anonymous** means that your identity will not be known and will not be attempted to be known.

  Reports made anonymously should include as much detail as possible, including any examples, so that investigations can be made thoroughly.

- Regardless if you choose to remain anonymous, information shared will be kept **confidential**.

  This means that the information about the person who made the report (if not anonymous), and any details about the situation/issue will only be shared with persons on a need-to-know basis and only to the extent allowed by law.

What Happens After Non-Compliance Is Detected?

Non-compliance must be investigated immediately and corrected promptly. Internal monitoring and auditing should ensure:

- No recurrence of the same non-compliance
- Ongoing CMS/DMHC compliance requirements
- Efficient and effective internal controls
- Protected enrollees

Internal monitoring activities include regular reviews confirming ongoing compliance and taking effective corrective actions.

Internal auditing is a formal review of compliance with a particular set of standards (for example, policies, procedures, laws, and regulations) used as base measures.

Reporting Non-Compliance

Reporting Options

- **IEHP's Compliance Toll Free Hotline: 866-355-9038**
- **E-Mail: compliance@iehp.org**
- **Fax: (909) 477-8536**
- **Mail:**

  IEHP Compliance Officer

  Inland Empire Health Plan

  P.O. Box 1800

  Rancho Cucamonga, CA 91729

- **Online Form:** Compliance Incident Report Form

IEHP
A Public Entity
Inland Empire Health Plan

Fraud, Waste and Abuse (FWA) Training

Training Objectives

- Understand the definitions and examples of FWA
- Learn about the FWA laws
- Understand your role for identifying and reporting FWA issues

Fraud, Waste and Abuse (FWA)

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* applies to practices that are inconsistent with sound fiscal, business, medical or recipient practices that result in unnecessary cost to a health care program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. Mistakes that are repeated after discovery or represent an on-going patter could constitute abuse.

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

Fraud, Waste and Abuse (FWA)

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

Fraud, Waste and Abuse (FWA)

Navigating the FWA laws

To detect FWA, you need to know the laws:

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

Fraud, Waste and Abuse (FWA)

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.

Fraud, Waste and Abuse (FWA)

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) §§ 3729-3733

Fraud, Waste and Abuse (FWA)

Health Care Fraud Statute

- "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 plead 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 plan.

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

Fraud, Waste and Abuse (FWA)

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.

Example

- Several doctors and medical clinics conspired to defraud by submitting claims for medically unnecessary power wheelchairs

For more information, refer to 18 USC § 1347.

Red Flags Examples

Fraud Red Flag	
	Obstructing an investigation or audit by withholding or delaying information or documentation
	A medical group alters documents to pass an audit by changing dates on a case file to give appearance of compliance to timeframes
	A nurse writes a verbal denial for a decision that was not made by the doctor

Fraud, Waste and Abuse (FWA)

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.
- Penalties include, but are not limited to:
  - Exclusion from participation in Federal health care programs
  - fine of up to $50,000 per kickback
  - Imprisonment

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).

Fraud, Waste and Abuse (FWA)

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
- Penalties include, but are not limited to:
  - Overpayment/refund obligation
  - Civil monetary penalties
  - Exclusion from participation in Federal health care programs

  Example
  - A California hospital was ordered to pay more that $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.
  - A provider refers a patient for a designated health service to a clinic where the physician (or an immediate family member) has an investment interest

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

Fraud, Waste and Abuse (FWA)

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
- Penalties depend on the specific violation and are subject to three times the amount:
  - Claimed for each service or item
  - 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 § 1128A(a) of the Social Security Act.

Fraud, Waste and Abuse (FWA)

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 System for Award Management (SAM), 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.

Fraud, Waste and Abuse (FWA)

Exclusion Example

A pharmaceutical company pleaded 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.

A hospital employs an excluded nurse who provides items or services to Federal health care program beneficiaries, even if the nurse's services are not separately billed and are paid as part of a Medicare diagnosis-related group payment the hospital receives

The excluded nurse violates their exclusion thereby causing the hospital to submit claims for items or services they provide

Fraud, Waste and Abuse (FWA)

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 § 1320a-7 and 42 Code of Federal Regulations (CFR) § 1001.1901.

Fraud, Waste and Abuse (FWA)

California State Laws

Welfare Institutions Code 14107 [False Claims]	Prohibits claim submission with intent to defraud to obtain greater compensation than legally entitled.
Welfare Institutions Code 14107 (a-b) [Anti-Kickback]	Solicits or receives any kickback, bribe or rebate to either refer or promise to refer person(s) for service or merchandise
CA Penal Code 550(a)(6-7) [False claims]	Imposes liability to knowingly make or cause to be made any false or fraudulent claim for health care benefit or which was not used by or on behalf of the claimant

Fraud, Waste and Abuse (FWA)

Knox-Keene Act

CA H&SC 1341 (a)	DMHC to ensure that health care service plans provide enrollees with access to quality health care services and protect and promote the interests of enrollees.
CA H&SC 1386 (b) (7) **[Fraud]**	Prohibits conduct that constitutes fraud or dishonest dealing or unfair competition, as defined by Section 17200 of the Business and Professions Code
CA H&SC 1371.37 [Claim payment]	A health care service plan is prohibited from engaging in an unfair payment pattern
CA H&SC 1367.02 [Economic Profiling]	Medical decisions are rendered by qualified medical providers, unhindered by fiscal and administrative management. Prohibits fraud of concealing or restricting costly specialists from network unless economic profiling policies disclosed to the DMHC

Please refer to the full Knox-Keene Act

Fraud, Waste and Abuse (FWA)

Combating FWA

Take action against FWA by following 3 steps:

- *Comply* with all applicable statutory and regulatory requirements, including implementing an effective compliance program.

- *Report* any compliance concerns, including suspected or actual violations of which you may be aware.

- *Conduct* yourself in a manner that aligns with the Code of Conduct.

Fraud, Waste and Abuse (FWA)

How Do You 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 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.

Fraud, Waste and Abuse (FWA)

Correction of FWA

- Once FWA is detected, promptly correct it. Correcting the problem saves money and ensures compliance with the 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.

Fraud, Waste and Abuse (FWA)

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?

Fraud, Waste and Abuse (FWA)

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?

Fraud, Waste and Abuse (FWA)

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 never picked up prescriptions?
  - 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)?

Reporting FWA Issues

Reporting Options

- **IEHP's Compliance Toll Free Hotline:** 866-355-9038
- **E-Mail:** compliance@iehp.org
- **Fax:** (909) 477-8536
- **Mail:**

  IEHP Compliance Officer
  Inland Empire Health Plan
  P.O. Box 1800
  Rancho Cucamonga, CA 91729
- **Online Form:** FWA Report Form

IEHP
A Public Entity
Inland Empire Health Plan

HIPAA Privacy & Security Training

Training Objectives

- Review HIPAA Privacy and Security
- Review key terms and definitions
- Understand when it's appropriate to access Member/Patient information
- Understand your role for identifying and reporting HIPAA Privacy and Security issues

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.

HIPAA: 4 Key Parts (Rules)

HIPAA Consists of four (**4**) key parts:

1. Privacy Rule
2. Security Rule
3. Breach Notification Reporting
4. Enforcement Rule

Important Dates in the History of HIPAA

- April 21, 1996 – HIPAA signed into law.
- April 14, 2003 – HIPAA Privacy Rule.
- April 21, 2005 – HIPAA Security Rule.
- February 17, 2009 – HITECH Act signed into law.
- August 24, 2009 – Breach Notification Rule.
- January 17, 2013 – HIPAA Omnibus Final Rule issued.

HIPAA *Privacy* Rule

- The Privacy Regulations went into effect April 14, 2003.
- Privacy refers to the protection of an individual's health care data.
- Defines how client information is ***used*** and ***disclosed***.
- Gives clients privacy rights (through a Notice of Privacy Practices or **NOPP**) and greater control over their own health information.
- Outlines ways to safeguard Protected Health Information (**PHI**).

HIPAA *Security* Rule

- Security regulations went into effect April 21, 2005.

Security means controlling:

- The confidentiality of electronic protected health information (**ePHI**).
- How client data is electronically stored.
- How client data is electronically accessed.

HIPAA *Breach Notification*

- The HIPAA Breach Notification Rule, **45 CFR §§ 164.400-414**, requires HIPAA covered entities and their business associates to provide notification following a breach of *unsecured* protected health information.

- Following a breach of unsecured PHI, covered entities must provide notification of breach to affected individuals, the Secretary (US Department of Health & Human Services) and, in certain circumstances, to the media.

- In addition, business associates must notify covered entities if a breach occurs at or by the *business associate*.

Definition of *Breach*

- A ***breach*** is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

- An impermissible use or disclosure of protected health information is presumed to be a breach, unless the **covered entity** or **business associate**, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a *risk assessment* of at least the following factors:

    1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    2. The unauthorized person who used the protected health information or to whom the disclosure was made;
    3. Whether the protected health information was actually acquired or viewed; and;
    4. The extent to which the risk to the protected health information has been mitigated.

Business Associate -- *Defined*

A ***business associate*** is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The Privacy Rule lists some of the functions or activities, as well as the services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information.

Business associate functions and activities include:

Claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Covered Entity-- *Defined*

- ***Covered entities*** are defined in the HIPAA rules as: (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

- Generally, these transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centers, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are covered entities.

- Covered entities can be institutions, organizations, or persons.

Refer to https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html for more information

HIPAA *Enforcement Rule*

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Rules, and procedures for hearings.

The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E.

HIPAA Fines and Penalties

Violation Category	Each Violation	All Identical Violations per Calendar Year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect - Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$1,500,000

HIPAA *Fines & Penalties*

1. The maximum civil penalty for knowingly violating HIPAA is $50,000 per violation up to a maximum of $1.5 million per violation category.

2. Criminal violations of HIPAA are handled by the DOJ (Department of Justice). As with the HIPAA civil penalties, there are different levels of severity for criminal violations.

3. Covered entities and specified individuals, as explained below, who "knowingly" obtain or disclose individually identifiable health information, in violation of the Administrative Simplification Regulations, face a fine of up to $50,000, as well as imprisonment up to 1 year.

4. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to 5 years in prison.

5. Finally, offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000 and imprisonment up to 10 years.

HIPAA *Enforcement*

- The Public. The public will be educated about their privacy rights and will not tolerate violations to their privacy! They will take action.

- Office For Civil Rights (***OCR***). This is the agency that enforces the privacy regulations. They will provide guidance and monitor compliance.

- Department of Justice (***DOJ***). This agency is involved in criminal privacy violations. Provides fines, penalties and imprisonment to offenders.

DEPARTMENT OF HEALTH & HUMAN SERVICES-USA
Office for Civil Rights

THE UNITED STATES DEPARTMENT of JUSTICE

HITECH Act (*expanded HIPAA*)

Health Information Technology for Economic and Clinical Health (HITECH) Act

- HITECH Act, enacted as part of the American Recovery and Reinvestment Act ARRA) of 2009.

- Addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen (expanded) the civil and criminal enforcement of the HIPAA rules.

    - Four categories of violations that reflect increasing levels of culpability;
    - Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation; and
    - A maximum penalty amount of $1.5 million for all violations of an identical provision.

HITECH Act (*cont'd*)

- Enforced by the Office of Civil Rights (OCR) of the Department of Health & Human Services.

- Additional enforcement is granted through state Attorneys General to order actions and obtain damages on behalf of individuals.

- HITECH applies HIPAA standards and penalties to Business Associates.

<u>Increased penalties for HIPAA Violations</u>:

- Maximum penalty per violation increases from $100 per violation to $50,000 maximum.
- The cap on penalties for all similar violations increased from $100,000 to $1,500,000.
- **Makes individuals subject to penalties**.

Protecting Information

- Health care entities must take steps to ensure that Member/Patient protected health information (PHI) is not viewed by anyone without "**a business need to know**," is not stolen, lost, or accidentally destroyed.

- Members/Patients be provided with rights over the use and disclosure of their own PHI.

- HIPAA covers health information in any form, including information that is stored or transmitted electronically.

Why do we need to comply with HIPAA?

- Member's Protected Health Information (PHI) is very sensitive and protected under privacy and information security laws.
- Keeping this data confidential, private, and secure is important to ensure:

    1. Preservation of trust of our members.
    2. Provision of quality health care.
    3. Compliance with federal/state regulations and internal policies.

Protecting Information

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.

HIPAA Definitions: *PHI*

PHI: Protected Health Information. PHI includes patient/member Identifiers.

Examples include:

Names
Medical Record Numbers
Social Security Numbers
Account Numbers
License/Certification numbers
Vehicle Identifiers/Serial numbers/License plate numbers
Internet protocol addresses
Health plan numbers
Full face photographic images and any comparable images

Web universal resource locaters (URLs)
Any dates related to any individual (date of birth)
Telephone numbers
Fax numbers
Email addresses
Biometric identifiers including finger and voice prints
Any other unique identifying number, characteristic or code

Protecting Information

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.

Use: when we review or use PHI internally (audits, training, customer service, quality improvement, billing).

Disclose: when we release or provide PHI to someone (ex. an attorney, a patient, faxing records to another provider, etc.).

Accessing PHI

The 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.

Protecting Information

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.

Protecting Information

Common PHI Violations

- 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 (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

Key Patients' Rights Under HIPAA

Patients have the following rights:

- Right to inspect and copy their PHI.
- Right to request to receive communication by alternative means or location.
- Right to Request an Amendment or Correct PHI.
- Right to Request a Restriction on use and disclosure of their PHI (ex. revoke a previous authorization, request to not give to certain providers, request to not provide for research purposes).
- Right to an Accounting of Disclosures of PHI.
- Right to receive NOPP (Notice of Privacy Practices).
- Right to file a privacy complaint.

Protecting Information

Information Security

Health care organizations are particularly vulnerable to cyber attacks. 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.

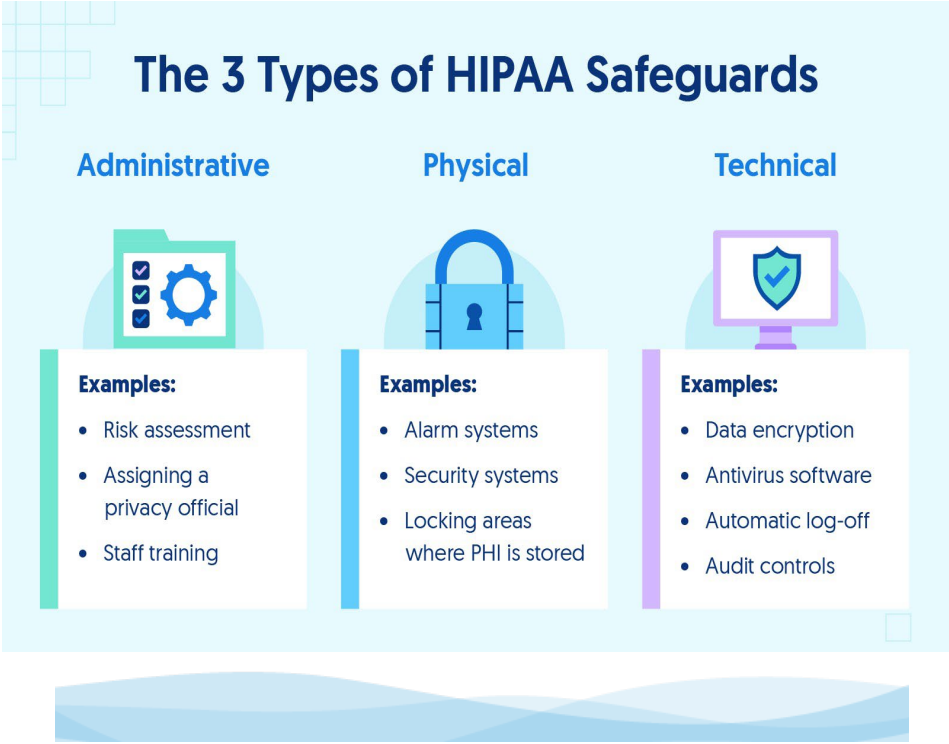
Protecting patients' data

One key element of protecting patients' PHI lies in maintaining the security of your systems, which houses and transmits ePHI (electronic protected health information).

The HIPAA Security Rule outlines how you need to do this.

How do you protect computer systems and your patients' information in them?

- By maintaining *Confidentiality*, *Availability*, and *Integrity* (**CIA**) of data you collect, store, create and by implementing and following various P&Ps required by the HIPAA Security Rule's three (3) Safeguards.



CIA triad

Definitions:

Confidentiality is a set of rules that limits access to information.

Integrity is the assurance that the information is trustworthy and accurate.

Availability is a guarantee of reliable access to the information by authorized people.

Breaking down the *CIA triad*

Confidentiality refers to protecting the privacy of PHI, ensuring this information is inaccessible to those unauthorized or without permission. Those allowed to access PHI are highly recommended to undergo Security Awareness training to equip them with the knowledge of potential security risks. When ensuring the confidentiality of PHI, businesses must have the appropriate technical, physical, and administrative safeguards in place, as outlined by the HIPAA Security Rule.

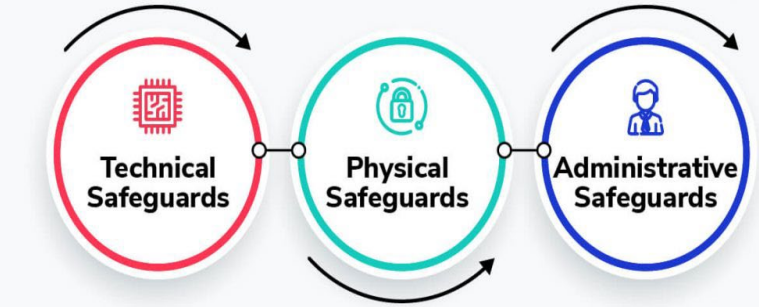
Maintaining the ***integrity*** of PHI is the act of maintaining its original quality and state, ensuring such data is not altered, manipulated, or destroyed by unauthorized users throughout its life cycle. Achieving this means adhering to the administrative and technical safeguards outlined by the HIPAA Security Rule. Businesses must have quality, trusted security systems in place to closely monitor any changes authorized or otherwise made to PHI.

Availability refers to an organization's ability to keep their hardware and software systems intact, and making sure PHI is easily accessible to those authorized to do so. Achieving this involves implementing the proper technical and physical safeguards. Using encryption software and having effective backup procedures are just a few basic security practices to keeping PHI intact. This guarantees such information stays readily available and unaltered in case of a security breach.

Applying HIPAA Security Safeguards

HIPAA requires for a covered entity to have ***there (3) Safeguards*** in place (i.e., organizational processes and corresponding policies and procedures).

Technical Safeguards	• Access Control • Audit Control • Integrity • Personal or Entity Authentication • Transmission Security
Physical Safeguards	• Security Management Process • Workforce Security • Information Access Management • Security Awareness and Training • Contingency Plan Evaluation • Business Associate Contract
Administrative Safeguards	• Facility Access Control • Workstation Use • Workstation Security • Device and Media Control



....And now, for some HIPAA *Do's* and *Don'ts*

- Never view patient records outside your scope of work. Only view records relevant to performing your job. No peeking/"snooping."
- Never share your ID or passwords with anyone and do not allow others to use the computer while you are logged in.
- Don't leave your password written down near your computer.
- Make certain to lock or lock-off your computer when you step away.
- Create strong, unique, and complex passwords.
- Use secure shredder bins to dispose of documents containing PHI or other confidential information.
- Never recycle documents containing confidential information (i.e., don't throw papers in your office trash can).

HIPAA *Do's* and *Don't (cont'd)*

- Keep PHI out of sight and secure it when not in use to prevent unauthorized access.
- Avoid patient-related discussions in public areas.
- Do not post PHI or other confidential information to social networking sites. This is a serious violation and constitutes a breach!
- If you emailing PHI to outside authorized parties, always use encryption.
- Do not email PHI to your personal email address.
- When faxing PHI to authorized parties, always use a Cover Sheet (don't put PHI in it). Make sure the number you are faxing is correct.
- Double/triple check it. Call the party you are faxing to, to make sure they received your fax.

Reporting Compliance Issues

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 Compliance Issues

Reporting Options

- **IEHP's Compliance Toll Free Hotline:** 866-355-9038
- **E-Mail:** compliance@iehp.org
- **Fax:** (909) 477-8536
- **Mail:**

  IEHP Compliance Officer
  Inland Empire Health Plan
  P.O. Box 1800
  Rancho Cucamonga, CA 91729

- **Online Form:** Privacy Incident Report Form

Summary

PRIVACY refers to WHAT is protected —information about an individual and the determination of WHO is permitted to use, disclose, or access the information.

SECURITY refers to HOW information is safeguarded—ensuring privacy by controlling access to information and protecting it from inappropriate disclosure and accidental or intentional destruction or loss.

Security is the key to protecting patients' privacy; a breach in security results in a breach of patient privacy.

All identifiable information about a patient is considered confidential. Sharing any of the confidential information inappropriately can result in a breach of patient confidentiality.

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.

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.