

# Annual Broker/Agent **General Compliance Training**

Protecting the Healthcare Investment

# Why Do You Need Training?

- **Sutter Health Plan (SHP) is required to review certain information with you every year.**
- **Brokers and agents must follow the laws and regulations that apply to our business.**
  - Healthcare laws and regulations change frequently
  - Existing policies are updated
  - New policies are developed
- **Every year billions of dollars are improperly spent because of Fraud, Waste and Abuse (FWA) and it affects everyone, including you.**
- **You are part of the solution.**

# Training Objectives

**At the end of this training, you will be able to:**

- Explain the purpose and importance of compliance
- Identify healthcare fraud, waste and abuse
- Understand fraud and abuse laws and consequences
- Understand key privacy and information security protections
- Recognize your role in safeguarding confidential information
- Report concerns

# Understanding Compliance

# What is Compliance and Why is it Important?

- Compliance is an organization's responsibility to adhere to all applicable laws, rules, policies, contractual obligations and business practices.
- Compliance programs are designed to implement compliance practices and internal controls to ensure the organization complies with applicable rules.
- Compliance practices help an organization prevent, detect and correct issues proactively rather than reactively.
- Compliance helps avoid mistakes and practices that could result in member complaints, negative publicity, audit findings, fines or even license suspension.
- Compliance can help prevent fraud, waste and abuse.

# The 7 Elements of a Compliance Program

**The fundamental elements of a compliance program are generally the same and include:**

1. Written Policies and Procedures and Code of Conduct
2. Compliance Leadership and Oversight
3. Training and Education
4. Effective Lines of Communication with the Compliance Officer and Disclosure Program
5. Enforcing Standards: Consequences and Incentives
6. Risk Assessment, Auditing, and Monitoring
7. Responding to Detected Offenses and Developing Corrective Action Initiative

For more information, refer to the [Office of Inspector General's General Compliance Program Guidance](#)

# Broker/Agent Role in Compliance



## Prevent

- Follow regulations and standards
- Do the right thing every time



## Detect

- Know regulations and standards
- Recognize potential compliance issues



## Report

- Report potential compliance issues
- Every broker/agent has an obligation to report questions and concerns about compliance issues



## What Should I Report?

Compliance training is to help you identify potential compliance issues by knowing what to look for.

*When in doubt, ask.*

## What Are Your Responsibilities?

**You are vital to prevent, detect and report non-compliance, as well as possible FWA.**

- You are required to comply with all applicable statutory, regulatory and other state and federal requirements.
- Make sure you are familiar with the SHP Code of Conduct and policies and procedures.
- Ensure you have policies and procedures in place that assist you in preventing, detecting, reporting and correcting issues of noncompliance and FWA.
- You have a duty to SHP to report any violations of laws that you may be aware of.



# Understanding FWA

# Purpose

SHP takes its responsibilities toward reducing cost, preventing waste and uncovering potential fraud very seriously. SHP empowers its brokers and agents to find, reduce, eliminate, or report fraud, waste and abuse (FWA).

This course will help you better understand what constitutes FWA and what you can do to prevent it.

Since FWA can happen in any part of our business, this course is important for everyone.



# Fraud

**Fraud** is an intentional or deliberate act to deprive another of property or money by deception or other unfair means.

For purposes of this training, fraud is defined as knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any healthcare benefit program; or to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any healthcare benefit program.

## **Examples of actions that may constitute fraud include:**

- Identity theft
- Marketing or sales techniques that coerce, mislead, or confuse potential enrollees
- Falsification of a member or employer group's information
- Bribery or kickbacks



## Waste

**Waste** is overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the health plan. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources.

**Examples of actions that may constitute waste include:**

- Conducting excessive office visits or writing excessive prescriptions.
- Prescribing more medications than necessary for the treatment of a specific condition.
- Ordering excessive laboratory tests.



## Abuse

**Abuse** includes actions that may, directly or indirectly, result in unnecessary costs to the health plan. 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.

**Examples of actions that may constitute abuse include:**

- Billing for unnecessary medical services.
- Billing for brand name drugs when generics are dispensed.
- Charging excessively for services or supplies.
- Misusing codes on a claim, such as upcoding or unbundling codes.

# Differences Between FWA



## Fraud

A primary difference is ***intent and knowledge***.

Fraud requires the person to have an intent to obtain payment and the knowledge that their actions are wrong.



## Waste & Abuse

May involve obtaining an improper payment but ***does not*** require the same intent and knowledge.

# Recognizing FWA

# Recognizing FWA in Healthcare

Now that you know what FWA is, you need to be able to recognize the signs of someone committing it. The following slides present potential FWA issues that may occur within a managed care organization. Each slide provides areas to keep an eye on, depending on your role in working with SHP and Sutter Health.





# Managed Care Organizations

## **Common Managed Care Organizations (MCO) violations include:**

- Use of deceptive, misleading or coercive marketing materials and tactics.
- Engaging in discriminatory marketing and enrollment.
- Un-enrolling or refusing to reenroll individuals needing costly services.
- Inappropriately withholding or delaying coverage of services.
- Failing to provide timely, accurate and complete data as required.
- Offering or accepting inappropriate discounts or kickbacks for the referral of government program business.

# Sales and Marketing

## Common Sales and Marketing violations include:

- Bribery and/or kickbacks — offering cash inducements to potential members to join a plan or insurer.
- Bait and switch — leading a potential member to believe that the cost of benefits are one price, only for the potential member to find out that the actual costs are higher once enrolled.
- Unlicensed insurance Broker/Agent.
- Failure to disclose information that can affect conditions of coverage.
- Selling nonexistent health plans or insurance policies.

# Conflicts of Interest

## Conflict of Interest

- A conflict of interest exists when an outside interest may influence or appear to influence your ability to be objective or to meet your broker or agent responsibilities.
- A conflict of interest is a type of fraud and can result in being unable to render impartial assistance or advice, having impaired objectivity, or an unfair competitive advantage in the business relationships of the company.

## Examples

- An agent selling a product for a company in which they have ownership regardless of the product meeting the need of the client or buyer.
- Steering beneficiaries into products that are not in their best interest.
- If you believe you may have a conflict of interest, discuss it with your broker or SHP.
- Conflicts of interest can sometimes be resolved if appropriate controls are put in place.

# Other Examples of FWA



## Potential Member Issues

- Member letting someone else use their ID card to receive medical services or medications.
- Identity theft.
- Doctor shopping.
- Adding individuals to a contract for coverage who are not eligible (e.g., lives and works outside the service area).
- Submitting forged or altered bills or receipts for reimbursement.



## Potential Provider Issues

- Billing for services not rendered and/or supplies not provided.
- Misrepresenting the dates services were rendered.
- Offering, soliciting, or receiving a bribe, kickback or rebate.
- Using unlicensed staff.
- Drug diversion.



## Potential Pharmacy Issues

- Drug shorting.
- Dispensing expired drugs.
- Prescription splitting.
- Billing for brand when generics are dispensed.
- Dispensing drugs that were not prescribed.

# Consequences for Committing FWA

# Consequences



**The following is a list of potential penalties depending on the violation:**

- Criminal conviction/fines
- Civil prosecution
- Imprisonment
- Loss of license to sell insurance
- Loss of license to practice medicine
- Exclusion from federal healthcare programs

# Laws and Regulations

**Fraud is constantly evolving. The following slides provide high-level information about some of the federal and state laws that are in place to combat FWA in the healthcare industry:**

- California Insurance Fraud Laws
- Civil False Claims Act, Health Care Fraud Statute, and Criminal Fraud
- Anti-Kickback Statute
- Exclusion

For details about the specific laws, such as safe harbor provisions, consult the applicable statute and regulations.

# Laws and Regulations

## California Insurance Fraud Laws

California's insurance fraud laws seek to prevent and punish false claims intended to generate payments to consumers or other payees of insurance companies.

*For more information refer to CA Insurance Code Sections 1871-1871.9*

### **Damages and Penalties:**

- Insurance fraud prosecuted as a misdemeanor in California may result in a sentence of up to one year in county jail, a fine of up to \$10,000, or both.
- Insurance fraud prosecuted as a felony can result in a term of imprisonment for two, three, or five years.
- Fines may be imposed in an amount up to \$50,000 or double the value of the defrauded amount, with the court choosing the greater of the two amounts.
- For many types of insurance fraud, a previous felony conviction for insurance fraud may result in a sentencing enhancement that adds two years for each prior offense to the defendant's term of imprisonment.
- Possible restitution to the victim.



# Laws and Regulations

## Civil False Claims Act (FCA)

The civil provisions of the FCA make a person liable to pay damages to the government if he or she knowingly:

- Conspires to violate the FCA;
- Carries out other acts to obtain property from the government by misrepresentation;
- Knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay the government;
- Makes or uses a false record or statement supporting a false claim; or
- Presents a false claim for payment or approval

*For more information refer to 31 United States Code (U.S.C.) Sections 3729-3733*

### **Damages and Penalties:**

- 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.
- The Civil Monetary Penalty (CMP) may range from \$5,500 to \$11,000 for each false claim.

# Laws and Regulations

## Health Care Fraud Statute

- The Health Care Fraud Statute states that “Whoever knowingly and willfully executes, or attempts to execute, a scheme to defraud any healthcare benefit program shall be fined or imprisoned not more than 10 years, or both”.
- Conviction under the statute does not require proof that the violator had knowledge of the law or specific intent to violate the law.

*For more information, refer to 18 U.S.C. Section 1346*

## Criminal Fraud

- Persons who knowingly make a false claim may be subject to criminal fines up to \$250,000; imprisonment for up to 20 years; or both.
- 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 U.S.C. Section 1347.*

# Laws and Regulations

## Anti-Kickback Statute

- The Anti-Kickback Statute prohibits knowingly and willfully soliciting, receiving, offering or paying remuneration (including any kickback, bribe or rebate) for referrals for services that are paid, in whole or in part, under a federal healthcare program (including the Medicare Program).

*For more information, refer to 42 U.S.C. Section 1320A-7b(b).*

### **Damages and Penalties:**

- Violations are punishable by a fine of up to \$25,000; imprisonment for up to 5 years; or both.

*For more information, refer to the Social Security Act, Section 1128B(b).*

# Laws and Regulations

## Exclusion

- No federal healthcare 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 healthcare programs and maintains the List of Excluded Individuals and Entities (LEIE).
- The United States General Services Administration (GSA) administers the Excluded Parties List System (EPLS), which contains debarment actions taken by various federal agencies, including the OIG.
- If looking for excluded individuals or entities, make sure to check both the LEIE and the EPLS since the lists are not the same.

*For more information, refer to 42 U.S.C. Section 1320a-7 and 42 Code of Federal Regulations Section 1001.1901.*

# Summary

- You play a vital role in preventing FWA.
- Make sure you are up-to-date with all applicable laws, regulations and policies.
- Verify information provided to you.
- Ensure data is both accurate and timely.
- Be on the lookout for suspicious activity.
- Promptly report potential FWA.

# **SHP Privacy and Information Security Training**

Brokers/Agents

# What is HIPAA?

## Health Insurance Portability and Accountability Act of 1996

- Privacy and information security of healthcare data.
- Created greater access to healthcare insurance.
- Promoted standardization and efficiency in the healthcare industry.
- Applies to Covered Entities (Health Plans, Health Care Clearing Houses, Health Care Providers, and Business Associates).

### **Damages and Penalties:**

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

*For more information, visit [hhs.gov/ocr/privacy](https://hhs.gov/ocr/privacy).*

# What is HITECH?

## Health Information Technology for Economic and Clinical Health

- Increased HIPAA enforcement
  - Department of Health and Human Services' Office of Civil Rights
  - State Attorney General
- Added significant penalties for HIPAA noncompliance
- Requires business associates to comply with HIPAA
- Expands individuals' rights to their own information
- Provides breach notification laws



# CA State Privacy Laws



## **Sutter Health is also regulated by state privacy and information security laws**

- These laws are often stricter than HIPAA and HITECH
  - More extensive requirements
  - Shorter breach notification standards & timelines
  - Enhanced fines and penalties for violations

*Please contact the SHP Privacy Officer or Information Security Officer if you have any questions regarding state privacy and information security regulations.*

# Safeguard What Information?

**Confidential Information Includes** data created, received, maintained or transmitted by or on behalf of SHP, and includes, but is not limited to:

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Member or Patient Information

Applies to All Formats of Information Sharing



Oral  
*Spoken*



Written



Electronic  
*ePHI*

# What is PHI?

**PHI is information that identifies the individual or could reasonably be used to identify the individual**

PHI is individually identifiable information, including demographic data, which relates to the:

- Individual's past, present or future physical or mental health or condition
- Healthcare provided to the individual
- Past, present or future payment for healthcare provided to the individual
- There are some limited exceptions, so reach out to the SHP Privacy Officer or Information Security Officer if you have questions.

# PHI

Protected Health Information is anything that can be used to identify an individual.

## PHI Identifier Examples



1. Electronic Email addresses
2. URL (Universal Resource Locator)
3. Internet Protocol (IP) address
4. Names of relatives
5. All elements of dates except year (DOB, admission, discharge, expiration, etc.)
6. Address (city, state, ZIP and geocodes)
7. Any vehicle VIN or other device serial number
8. Fax number
9. Certificate or license number
10. Photographic images
11. Fingerprints or voiceprints
12. Telephone numbers
13. Name
14. Social Security number
15. Health plan beneficiary number
16. Medical record number
17. Account number
18. Any other unique or identifying number, characteristic or code

# Examples of PHI Data

- Account Number
- Address (city, state, ZIP, and geocodes)
- All elements of dates except year (DOB, admission, discharge, expiration, etc.)
- Alternative Member Identifier (AMI)
- Benefit Coverage Information
- Certificate/License Numbers
- Claim Numbers/Data
- Date of Service
- Device Identifiers
- Eligibility/Enrollment Data
- Email and IP Address
- Employer's Name
- Finger and Voice Prints
- Full Face Photo
- Health Plan Beneficiary Numbers
- Medical Information (Medical Records, Lab Values, Health Risk Assessments)
- Medical Record Number
- Name
- Names of Relatives and Employers
- Photographic images
- Social Security Number (SSN)
- Telephone and/or Fax Numbers
- URL or Web Address
- Vehicle Identifiers and Serial Numbers
- X-Rays

# Protecting PHI

The data in the previous slide could be PHI either alone, or if combined, would allow for an individual to be identified.

Examples of information SHP brokers and agents hold:

- ZIP Code alone **WOULD NOT** be PHI, but combined with address and phone number would be PHI; the combination of these data elements could be used to identify an individual.
- Birth Date alone **WOULD NOT** be PHI, but combined with a name could result in identification of an individual and would be considered PHI.
- Social Security Number alone **WOULD** be PHI as this data element can be used to identify an individual.

*The context and combination of the data elements will determine whether information is PHI. If you have any questions about what is or is not PHI, check with the SHP Privacy Officer or Information Security Officer.*

# Why Protect PHI?

**Penalties may be imposed for improperly using, accessing or disclosing PHI.**

- An individual can be criminally liable for violating HIPAA and HITECH laws.
- Audit by Department of Health and Human Services or other state and federal agencies resulting in fines and other penalties.
- Corrective action up to and including termination.

# Protecting PHI

## Protecting PHI

### Safeguarding Protected Health Information

- Brokers and agents must employ the appropriate administrative, technical and physical safeguards to protect the privacy of protected health information.

### Use and Disclosure of Information

- Member information cannot be disclosed to others without the individual's written authorization except for the purposes of treatment (providing care), payment (claim payment) or health plan operations (examples include, but are not limited to, audits and fraud and abuse detection).



# Protecting PHI

## Requirements for Protecting PHI

### Minimum Necessary

- When collecting, accessing, using or disclosing PHI, brokers and agents must make reasonable efforts to limit the use and disclosure to the minimum necessary to accomplish the intended purpose.

### Theft Prevention

- Never leave laptops, paper PHI, or other devices containing member PHI in a vehicle unattended; electronic devices are especially attractive to thieves.

# Protecting PHI

## Frequently Asked Questions Regarding Transmitting PHI

### PHI Sharing via the Internet

- Per Business Associate Agreement, email communications must utilize an email encryption process.

### PHI Sharing via Fax

- Stop, pause and double check you are dialing the correct fax number.
- Report all misdirected faxes immediately through the SHP Privacy Officer or Information Security Officer, the Sutter Health Confidential Message at 800-500-1950 or via the online form at [sutterhealth.org/report-it](https://sutterhealth.org/report-it).

# Protecting PHI

If a broker or agent becomes aware of a potential violation of the HIPAA Privacy Rule, Security Rule or HITECH Act, or any state privacy or information security law, report this immediately to the SHP Privacy Officer or Information Security Officer.

## What Can I Do to Protect PHI?

- Pick up documents from copiers, printers, and fax machines right away.
- Dispose of documents containing PHI in locked shred bins when no longer needed.
- Stop, pause and double check contact information before sending a fax or email.
- Encrypt all PHI emails you send.
- Lock up paper PHI.
- Lock your computer when leaving.
- Do not leave devices or paper containing PHI unattended.
- Ensure all passwords and passcodes are unique and strong.
- Contact the SHP Privacy Officer or Information Security Officer as soon as a concern arises.
- Implement Best Practices for Using, Accessing, and Disclosing PHI.

# How Do I Report Concerns?

# Sutter Health Plan Officers

The best way to report issues, if you're comfortable doing so, is to report the issue directly to the SHP Ethics & Compliance Officer, Privacy Officer or Information Security Officer; it helps us know who to go to if additional information is needed to resolve the issue.



**Trisha Burgos**

SHP Ethics & Compliance Officer  
[Trisha.Burgos@sutterhealth.org](mailto:Trisha.Burgos@sutterhealth.org)  
916-643-1321



**Braden Carkhuff**

SHP Privacy Officer  
[Braden.Carkhuff@sutterhealth.org](mailto:Braden.Carkhuff@sutterhealth.org)  
916-300-4199



**Kelly Garfield**

Information Security Officer  
[Krystine.Garfield@sutterhealth.org](mailto:Krystine.Garfield@sutterhealth.org)  
916-871-9610

# Other Ways to Report Concerns

**Report the issue to any SHP leader (manager/director/VP)**

**Contact SHP Customer Service: 855-315-5800**

**Call the Confidential Message Line: 800-500-1950**

- An external company manages our Confidential Message Line, which has been designed to make it easy for you to report any issue or instance of misconduct.
- An operator is available 24/7.
- You can also submit your concern online at [sutterhealth.org/report-it](https://sutterhealth.org/report-it).

**Email: [shpcompliance@sutterhealth.org](mailto:shpcompliance@sutterhealth.org)**

**Mail:**

Sutter Health Plan  
Attn: Compliance Officer  
P.O. Box 160307  
Sacramento, CA 95816

# Reporting FWA

**You can report suspected FWA using any of the reporting methods.**

**If you are submitting your report by mail or email, please complete the Suspected Fraud and Abuse Reporting Form or include the following information in your report:**

- Date suspected fraud occurred
- Date suspected fraud was discovered
- Where the suspected fraud occurred
- A description of the incident or suspected fraud
- A list of all persons engaged in the suspected fraud
- How you became aware of the suspected fraud
- A list of any individuals who have attempted to conceal the issue, and the steps they took to conceal it



# Congratulations!

You have completed the Sutter Health Plan Fraud, Waste, and Abuse and General Compliance Training.

To receive credit for this training, please submit the **attestation form**.