



# Corporate Compliance Plan

2025 Annual Safety and Compliance Training (ASCT)

## **Core Learning Objectives of this course:**

Our Corporate Compliance Program is designed to ensure Methodist Health System (MHS) and our workforce members follow federal, state, and local laws and regulations, as well as internal policies and procedures.

Our Compliance Program:

- Demonstrates MHS's commitment to responsible and honest business conduct
- Encourages employees to report potential problems
- Increases the likelihood of preventing, identifying, and correcting unlawful conduct
- Helps mitigate damage in cases of non-compliance

**The Corporate  
Compliance  
program has  
two main  
parts.**

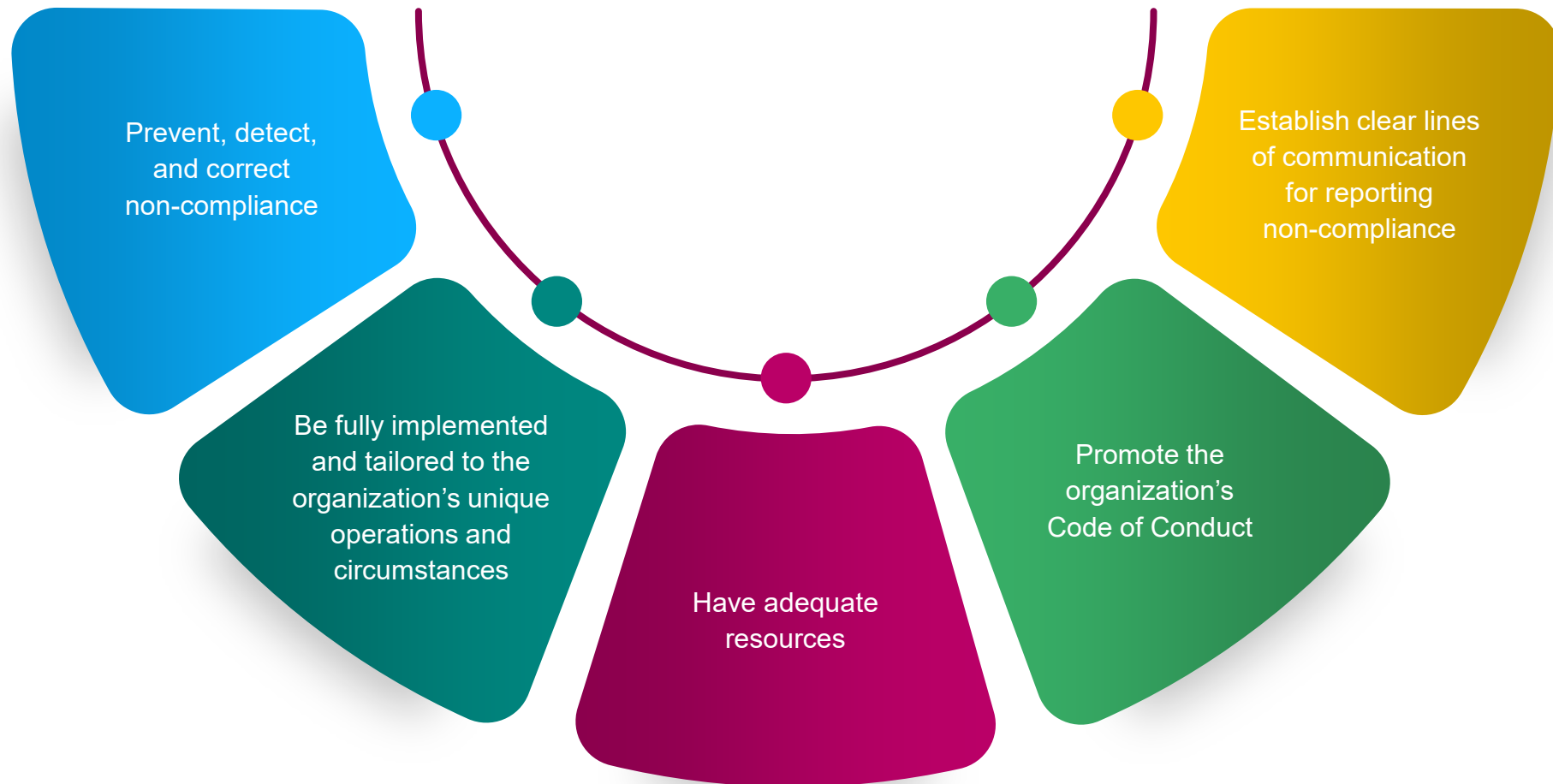
**01**

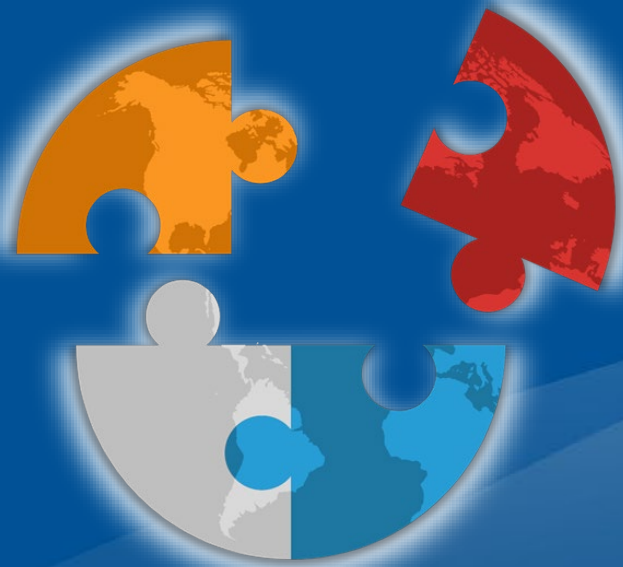
**Corporate  
Compliance Plan**

**02**

**Code of Conduct**  
You will learn more about  
this in another course.

## An effective compliance program must foster a culture of compliance within an organization and, at a minimum:





For our compliance program to continue to be successful, every MHS employee and agent needs to understand their responsibility to support the culture of compliance.

It's crucial that we do not personally, or as an organization, engage in any inappropriate or illegal behavior.

**Our  
Compliance  
Program**

**Demonstrates MHS's commitment  
to responsible and honest  
business conduct**



**Encourages employees to report  
potential problems**



**Increases the likelihood of  
preventing, identifying, and  
correcting unlawful conduct**



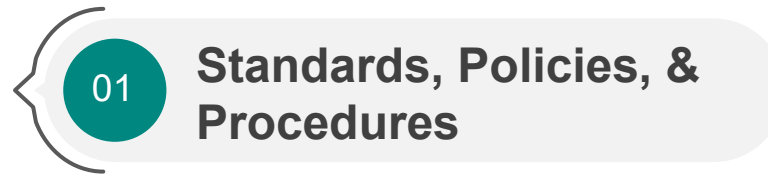
**Helps mitigate damage in cases  
of non-compliance**



# The Corporate Compliance Plan consists of seven elements.

These 7 Elements are based on recommendations from the Office of Inspector General (OIG) and are identified in the US Sentencing Guidelines as essential to an effective compliance program.



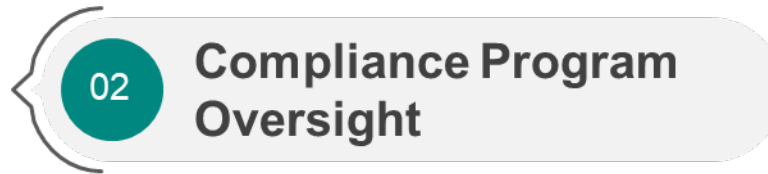


## 01 Standards, Policies, & Procedures

The foundational documents of the Corporate Compliance Program are the Corporate Compliance Plan and the Code of Conduct, which are designed to provide guidance to employees on what is and is not appropriate behavior. Other standards, policies, and procedures may take different forms. Examples include Compliance Department policies and procedures, Human Resources policies and procedures, and individual department policies.

Particular emphasis has been placed on the areas of financial billing, accreditation, conflicts of interest, physician relationships, quality of care, research, gifts, confidentiality, non-discrimination, and organizational ethics.





## 02 Compliance Program Oversight

The Audit and Compliance Committee of the MHS Board of Directors has been delegated oversight over the Corporate Compliance Program. The MHS Board appoints the Chief Compliance Officer; adopts and implements the Corporate Compliance Program and related policies, procedures, monitoring, and enforcement; and exercises final authority on all compliance matters.

The Corporate Compliance Program is overseen by the Vice President of Compliance/MHS Corporate Compliance Officer and the Chief Compliance Officer. The Vice President of Compliance will also delegate authority to assist with oversight activities.

02

## Compliance Program Oversight

**Shari Flowers**, General Counsel & VP Compliance

**Jen Anderson**, Chief Compliance Officer

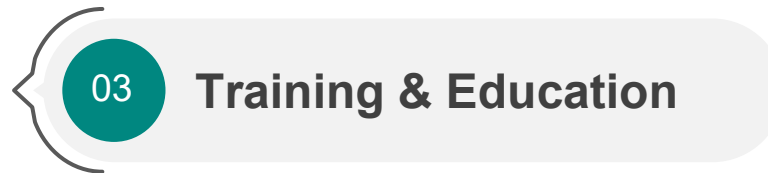
**Anita Patterson**, Privacy Officer

**Lyndsay Lang**, Employee Relations Consultant

**Michael Kearns**, Director Information Security



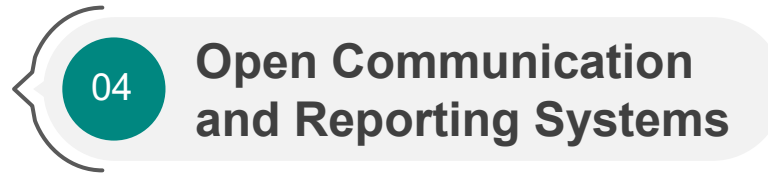
**Who do I  
contact for  
compliance  
issues?**



## 03 Training & Education

MHS has various policies and educational programs designed to teach personnel about the Corporate Compliance Program. It is the responsibility of all employees and agents of MHS to be knowledgeable about the compliance requirements of their specific positions.

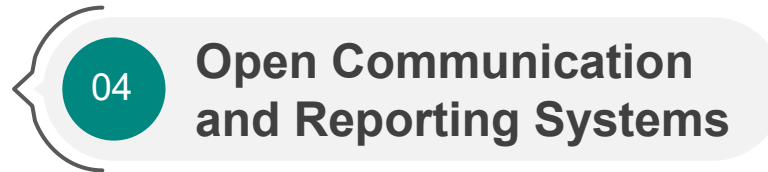
This course provides basic compliance training, and it is supplemented with articles in employee and management newsletters and live, on-site training designed to enable discussion and full understanding of complex regulations for each department based on the specific risks associated with job duties. For additional compliance training, please talk to your supervisor or contact the Compliance Department.



## 04 Open Communication and Reporting Systems

All employees and agents of MHS who have firsthand knowledge of activities or omissions that may violate applicable laws, regulations, the Code of Conduct, policies, or professional standards have an affirmative obligation to report such wrongdoing.

**No employee or agent making a good faith report will be retaliated against by MHS or any of its affiliates, employees or agents.**



## 04 Open Communication and Reporting Systems

Everyone is encouraged to contact their Supervisor or the Compliance Department for clarification or direction regarding the Corporate Compliance Program.

If you have a concern or knowledge of a violation of applicable laws or regulations, you are required to report such activity.

**No retaliation will be permitted against an employee making such a report.** Employees making reports are encouraged to disclose their identity to allow a full and timely investigation of the concerns, however, anonymous reporting is an option. No report will be refused or treated less seriously because the reporter chooses not to be identified.

04

## Open Communication and Reporting Systems

### Reporting Compliance Issues:

#### *See Something? Say Something!*

Reporting is available for any Fraud, Compliance & Ethics, or Human Resource issue. Reporting is confidential and always available through an independent third party.



#### COMPLIANCE HOTLINE

1-877-640-0005 (English)

1-800-216-1288 (Spanish)

[www.lighthouse-services.com/nmhs](http://www.lighthouse-services.com/nmhs)





05

## Monitoring & Auditing

**Monitoring** is the process of continuously or periodically checking performance of staff and/or systems to ensure they are working efficiently and effectively and in compliance with all applicable laws and regulations.

**Auditing** is the oversight process used to review procedures, systems, and processes. Auditing across MHS is conducted by the Internal Audit department, an independent department dedicated to evaluating and improving the effectiveness of the risk management, internal control, and corporate governance processes while adding value by improving operation and process efficiency.

**Monitoring & Auditing Activities are reported through these various Compliance Committees:** OIG Work Group, Operational Compliance, Corporate Compliance.



06

## Corrective Action Plans

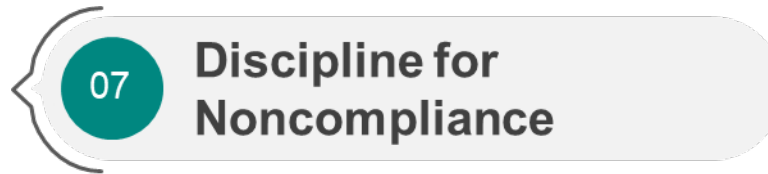
Any compliance issues that are reported or discovered will be promptly and fully investigated by the Compliance Department.

Following an investigation, the Compliance Department, in coordination with relevant departments and supervisory personnel, will take whatever corrective actions are necessary and appropriate to make sure we are in full compliance with all applicable laws and regulations and to prevent further, similar violations.

Corrective action may include:

- Updates to policies and procedures
- Staff re-education
- Disciplinary action
- System and/or process redesign





07 Discipline for Noncompliance

**Anyone who knowingly violates MHS policy is subject to disciplinary action.**

This may include documented discussion, written warning, suspension, termination, suspension of the right to access the MHS IT Network, and/or termination of other privileges.

Depending on the circumstances and severity of the issue, MHS may also notify law enforcement officials and/or regulatory, accreditation, and licensure organizations.

07

## Discipline for Noncompliance

### **Examples of inappropriate and/or illegal behavior include:**

- Falsifying, forging, or altering records, bills, or other documents
- Stealing or misusing funds, supplies, property, and/or other MHS resources
- Accessing or altering computer files or patient records without authority
- Falsifying reports to management or external agencies
- Violating the MHS Conflict of Interest policy
- Storing patient information on unsecured mobile/portable devices
- Failing to comply with OSHA guidelines
- Accessing or sharing confidential information without a need-to-know
- Inappropriately accessing or using protected health information



# HIPAA

2025 Annual Safety and Compliance Training (ASCT)

## **Core Learning Objectives of this course:**

**Upon completion of the privacy training, you will understand the important elements of HIPAA:**

- HIPAA and various regulations that apply to your job
- The significance of incident reporting and the potential sanctions associated with breaches
- The safety and security protocols in place to adhere to HIPAA
- How PHI is used and disclosed at Methodist

# Privacy Officer Role:

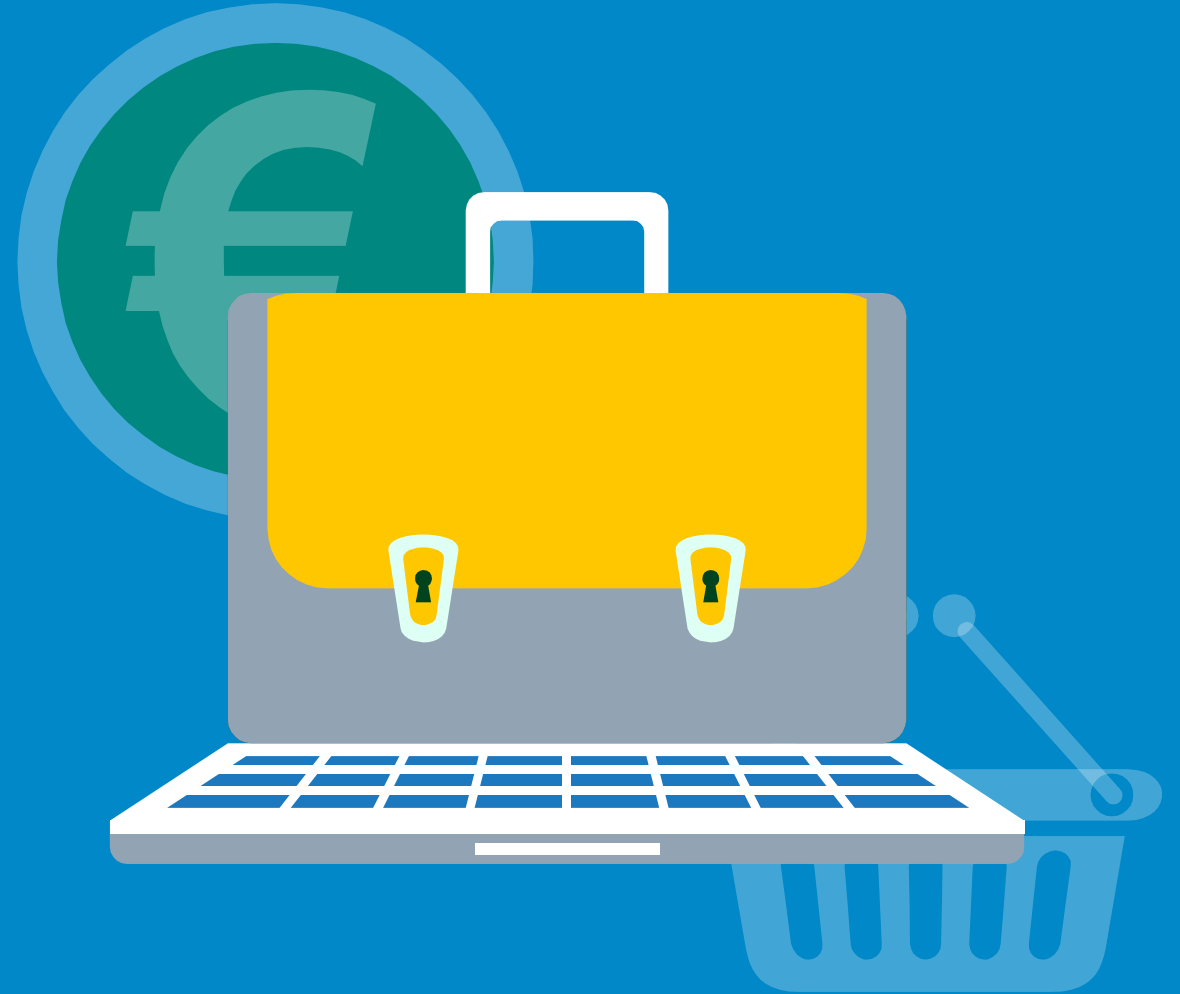
**The Privacy Officer serves as the first point of contact for all issues related to HIPAA privacy and security at Methodist Health System. The functions of the Privacy Officer include:**

- Maintain high standards for the privacy and security of our patients' and workforce health information.
- Promote a culture of privacy and confidentiality within the health system.
- Monitor the privacy and security of health information throughout the health system.
- Receive and respond to questions from our patients and workforce concerning the use and disclosure of health information.
- Support the Methodist Health System efforts for HIPAA compliance as well as other laws/regulations regarding data privacy and security.
- Lead data breach response and notification efforts.
- Liaise with Information Security regarding data privacy and security issues.
- If you have any questions or concerns about privacy issues, please contact MHS Privacy Officer, Anita Patterson at (402)354-6863/anita.patterson@nmhs.org or the Compliance Reporting Hotline at (877)640-0005 (English) or (800)216-1288 (Spanish). Both options are 100% confidential.
- For suspected Information Security Incidents, contact the ITOC promptly at (402)354-2280.

# Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act, and the associated Privacy and Security Regulations, apply to almost every organization or person that provides or pays for health services or exchanges health-related information.

Failure to abide by HIPAA rules and regulations can lead to increased healthcare costs, civil monetary penalties, lawsuits, and disciplinary action.






## Health Insurance Portability and Accountability Act (HIPAA)


The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rule protects the privacy and security of health information and gives individuals rights to their health information. HIPAA establishes standards for covered entities and their business associates to safeguard the Protected Health Information (PHI) of patients.

# This HIPAA training will discuss:




The Privacy Rule, which sets national standards for the use and disclosure of PHI

01



The Security Rule, which specifies safeguards that covered entities and their business associates must use to protect the confidentiality, integrity, and availability of electronic protected health information (e-PHI)

02




The Breach Notification Rule, which requires covered entities to notify affected individuals, the department of Health and Human Services, and, in some cases, the media of a breach of unsecured PHI.

03




## This HIPAA training will discuss:



The Omnibus Rule,  
Ensure business  
associates are  
aware of  
HIPAA safeguards.

04



The Enforcement Rule,  
focuses on how HIPAA  
rules are applied to  
enforce investigations  
of potential  
violations and  
enforcing penalties.

05

The Privacy Rule protects PHI held or transmitted by a covered entity or its business associates, in any form, whether electronic, paper, or verbal. Records containing PHI need to be secured so they are not readily available to those who do not need to see them. Records are to be accessed on a “need to know basis” or within one’s job scope.



## Protected Health Information (PHI) includes:

01



Common identifiers, such as name, address, birth date, and Social Security Number

02



Information about past, present, or future physical or mental health or conditions.

03



Information about the provision of health care to the individual.

04



Information about the past, present, or future payment for the provision of health care.

# The Privacy Rule distinguishes between the use or disclosure of PHI:

## Use

When PHI is used internally for Treatment, Payment, or other Healthcare Operations (audits, training, customer service, internal analysis, etc.).

## Disclosure

To release or provide access to a patient's PHI to someone like a physician, an attorney, insurance company, etc., outside of Methodist Health System.

**Protected Health Information (PHI):** There are 18 specific identifiers that must be removed from any information set for the information to be considered de-identified.

# Specific identifiers that must be removed from any information set for the information to be considered de-identified:

1

- Names

2

- Address

3

- Any dates (except years) that are directly related to the individual

4

- Telephone Numbers

5

- Fax Numbers

6

- Email addresses

7

- Social Security numbers

8

- Medical Record numbers

Specific identifiers that must be removed from any information set for the information to be considered de-identified:

9

- Health Plan beneficiary numbers

10

- Account numbers

11

- Certificate/license numbers

12

- Vehicle identifiers and serial numbers, including license plate numbers

13

- Device identifiers and serial numbers

14

- Web universal resource locators (URLS's)

15

- Internet protocol (IP) address numbers

16

- Biometric identifiers, including finger and voice prints

Specific identifiers that must be removed from any information set for the information to be considered de-identified:

17

- Full face photographic images and any comparable images

18

- Any other characteristic that could uniquely identify the individual

**HIPAA's Privacy Regulations apply to almost every organization or person that provides or pays for health services or exchanges health-related information, including:**

- Physicians
- Nurses
- Health care facilities (and people who work there)
- Health Plans
- Any other organization/person that handles PHI
- Business associates (any company that has access to, or uses, PHI in order to perform a service for a doctor, nurse, hospital, or other covered entity)



**Confidentiality** is the safekeeping of information by individuals who have a need, reason and permission to access such information. The MHS Confidentiality Policy states:

- **Employees with access to confidential patient, employee, and/or proprietary information have a duty to maintain the confidentiality of all information obtained during employment and after employment.**
- This includes patient medical, personal, and financial information.
- Local, state, and federal laws protect the confidentiality of such information, and employees will be personally liable for any breach of this duty.
- Releasing confidential information without permission may result in disciplinary action, suspension, and/or termination. Employees are accountable for their actions on and off duty.



**Notifying your supervisor if someone requests to have a patient's chart duplicated.**

**Only discussing patient information in areas where other patients, visitors, and employees cannot overhear.**

**Protecting Patient Confidentiality Includes:**

**Releasing verbal and/or written information only with proper or written consent.**

**Directing reporters/news media to Methodist Marketing/Public Relations, if they are requesting information about a patient.**

## Accessing Your Own or Your Family Members' Medical Records



MHS employees may not access their family members' or their own electronic medical records. Employees are encouraged to sign up for the Methodist My Care Patient Portal. Methodist My Care is a secure online portal that can help patients manage their health information. Please visit the [Methodist My Care page](#) for additional information.



MHS physicians (MD's and DOs) may access the electronic medical records of their dependent minor children without a written authorization. Physicians may also access the electronic medical records of a family member who is not a dependent minor with a valid, signed Physician Authorization Form scanned in Cerner.

## HIPAA Privacy Rule: Under HIPAA, patients have a right to:



Right to receive a copy of the Notice of Privacy Practices (NPP), even if they have previously received it electronically



Right to inspect records and receive a copy of their medical records, including an electronic copy of their electronic medical records



Right to request a correction or amendment if they believe their medical record is inaccurate



Right to request an alternative means of communication or choose how PHI is received



Right to opt-out of the facility directory if an inpatient



Right to request a restriction on the use or disclosure of PHI



Right to receive an Accounting of Disclosures - Patients can request a list of all parties to whom we have released PHI



Right to file a complaint without fear of discrimination or retaliation

## **HIPAA Privacy Rule**

Under the Privacy Rule, patients can restrict their health plan's access to information about treatments they paid for in cash, and most health plans cannot use or disclose genetic information for underwriting purposes.

## Notice of Privacy Practices

The Notice of Privacy Practices is displayed in a prominent location and made available to all patients to help patients understand their rights under HIPAA. The Notice of Privacy Practices informs the patients of:



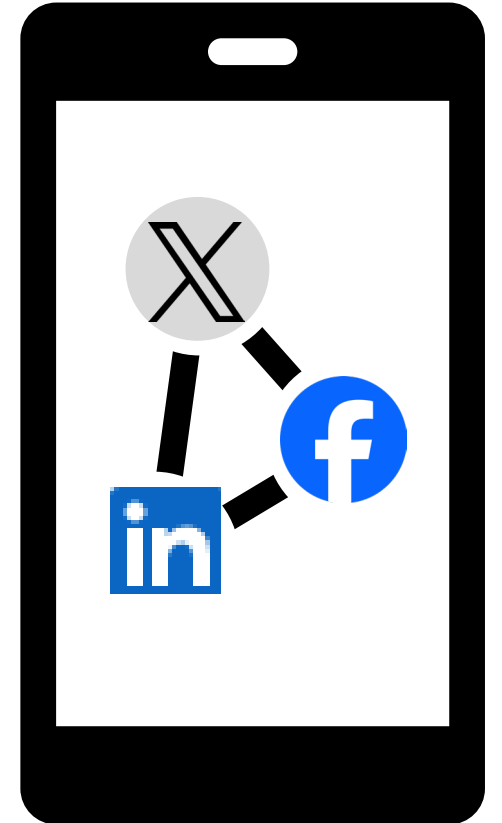
## HIPAA and Social Media

HIPAA, prohibits the use and disclosure of protected health information (PHI) on social media, this means healthcare professionals must be extremely cautious about what they share – disclosing PHI without consent is a HIPAA violation. This includes names, photos and any information that could identify a patient or their medical condition. Inappropriate posts can seriously damage Methodist Health System's reputation.

### ***Examples of HIPAA violations on social media:***

- Discussing patient cases on personal social media accounts, even in a general way
- Failing to obtain proper authorization before posting patient testimonials or stories – MHS Marketing Department will help you share your testimonials in a HIPAA compliant manner
- Posting a fun photo of yourself and a coworker from your workplace without discretion could unintentionally capture a patient, a family member, or sensitive patient information in the background.
- Friending patients on social media and engaging in medical discussions with patients
- Commenting on a patient's health status or treatment, even if initiated by the patient
- Sharing information that could indirectly identify a patient, such as their room number or diagnosis

**Note:** Searching for patients on social media is not automatically a breach of ethics; however, concerns arise when healthcare professionals utilize information obtained from these searches to influence patient care decisions or share details with others without the patient's consent. Always prioritize providing patient care based on the information shared by patients while they are in your care.

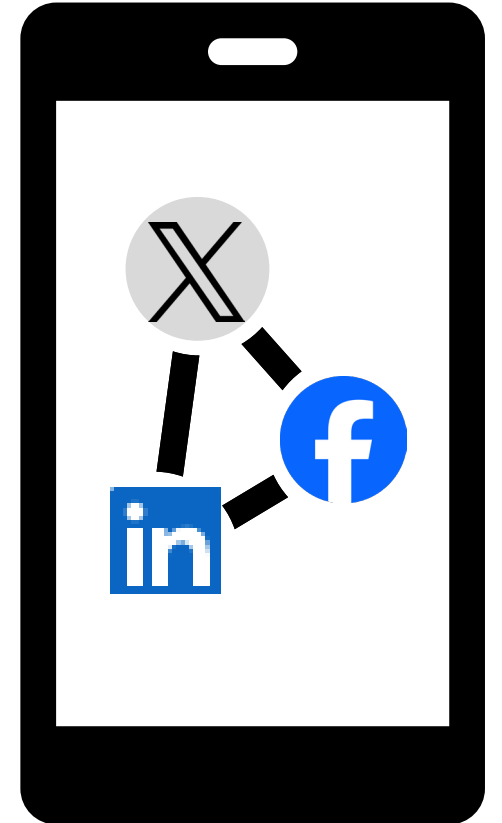


## HIPAA Social Media

### *Consequences of HIPAA violations*

- Fines and penalties for the healthcare organizations and potentially for individuals involved
- Loss of reputation and public trust
- Violation of the social media policy may result in disciplinary action, which may include suspension, restriction of access, or termination of employment

All employees are expected to conduct themselves in a manner that reflects integrity, as well as shows respect and concern for others, including the use of social media.





The Security Regulation applies to the same entities as the Privacy Regulation.

The Security Rule specifies safeguards that covered entities and their business associates must use to protect electronic protected health information (e-PHI). We must:



Ensure the confidentiality, integrity, and availability of e-PHI

**Confidentiality:** e-PHI cannot be available or disclosed to unauthorized persons

**Integrity:** e-PHI cannot be altered or destroyed in an unauthorized manner

**Availability:** e-PHI must be accessible and usable on demand by authorized persons



Identify and protect against reasonably anticipated threats to the security or integrity of the information



Protect against reasonably anticipated, impermissible uses or disclosures. We do this by maintaining reasonable and appropriate administrative, physical, and technical safeguards.

## Administrative Safeguards

We are required to implement administrative safeguards to identify, analyze, and mitigate risks to e-PHI.

### How do we do this?

- IT security personnel
- Information security policies and procedures
- Information security training

The IT security staff develops policies and procedures, monitors systems, tests processes, and trains employees.

Failure to follow information security policies or complete required training will result in disciplinary action.

## Personal Use

Authorized internet and email users must use good judgment regarding the reasonableness of personal use. MHS management reserves the right to define and approve what constitutes reasonable personal use.

Personal use of MHS Electronic Resources must never interfere with work or the ability of MHS to use its resources for business purposes. Prior use of a MHS Electronic Resource for personal use does not necessarily constitute continuing approval.



## Personal Use

**All personal use must be consistent with the Information Security Policy and the highest standards of ethical conduct.** Personal use must not violate policies, statutes, contractual obligations, or other standards of acceptable behavior.

**Under no circumstances may an MHS user engage in any activity that is illegal** under local, state, federal or applicable international law while using MHS Electronic Resources. Refrain from unauthorized viewing or use of another person's account, computer files, programs, and/or data. Access to such information does not imply permission to view or use it.

MHS systems may not be used to solicit business, sell products, or otherwise engage in commercial activities unless expressly permitted by MHS management. Except as authorized by MHS, use of MHS systems or data for personal business, political campaigning, or other commercial purposes is prohibited.

MHS email, instant messaging or other electronic communications systems may not be used to create or distribute any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Users must not create or disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

**If you receive offensive email from another employee, please immediately report the matter to your manager or the Compliance Hotline at (877)640-0005 (English), (800)216-1288 (Spanish), or [www.lighthouse-services.com/nmhs](http://www.lighthouse-services.com/nmhs).**



**Any email you send *could* be forwarded on to others without your knowledge or consent.** All emails sent or forwarded outside of the MHS network have a Privacy and Intended Use Disclaimer footer, but it's a good idea to use caution whether you're emailing internally or externally. You should encrypt outgoing emails containing PHI or other private information by adding the word "encrypt" anywhere in the subject line.

**Any email you send *could* be forwarded on to others without your knowledge or consent.** All emails sent or forwarded outside of the MHS network have a Privacy and Intended Use Disclaimer footer, but it's a good idea to use caution whether you're emailing internally or externally.

## **All digital communication is trackable!**

MHS will routinely send you test phishing e-mails to see if you are paying attention and properly screening for phish attempts. If you fail the phishing test, you will be assigned mandatory training.

Failure to complete the assigned training after failing our random phishing test will result in disciplinary action up to and including work suspension or termination.

Anyone who violates MHS policy faces corrective action based upon the MHS *Behavioral Improvement/Corrective Action Guidelines* and *Sanctions for HIPAA Violations* policies.

**Sanctions may include, but are not limited to:**

Verbal or written  
warning

Suspension

Termination

Suspension of the right  
to access the MHS IT  
Network and/or  
termination of other  
privileges.



***MHS may also notify law enforcement officials, and regulatory, accreditation, and licensure organizations.***

Verbal or written  
warning

Suspension

Termination

Suspension of the right  
to access the MHS IT  
Network and/or  
termination of other  
privileges.

**Physical Safeguards** are controls for facility and workstation access. Facility access is controlled by our use of name badges with employee photos and security badge scanners on doorways that lead to areas containing PHI.

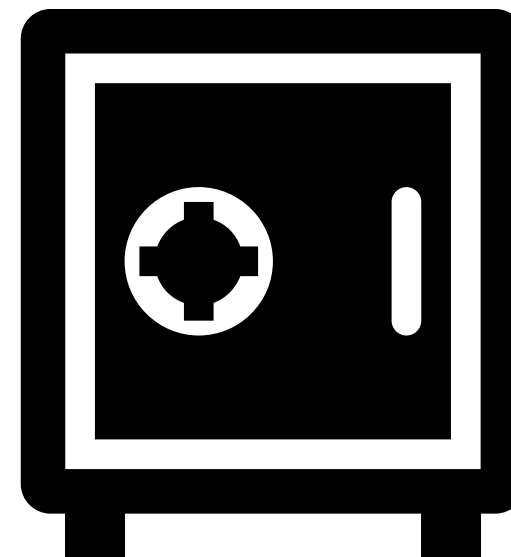
Workstation access is controlled by a combination of facility access and staff diligence. You can do your part to protect PHI, and other private and confidential information, by keeping access-controlled doors closed, picking up your documents from printers right away or using secure printing (print hold), and always using a shred bin when you're done with a document. To ensure the security of sensitive documents awaiting shredding, be sure you insert the paper all the way into the bin.

## Technical Safeguards

Technical safeguards are the systems MHS IT has put into place to implement access controls for e-PHI, to monitor and/or audit Information Systems, and to establish our network and secure all network traffic.

We also have controls in place to back-up critical data and ensure that e-PHI is not improperly altered or destroyed.

Any data kept on any Information System is the property of MHS. This information, including emails, may be examined by MHS employees or designees at any time, without notification, and used in any acceptable manner.



MHS IT systems record and monitor access to our systems, including CERNER, information security incidents, events and weaknesses.

**MHS reserves the right to monitor and record the usage of all computing resources as necessary to evaluate and maintain system efficiency, ensure compliance with MHS policies and applicable laws and regulations, and monitor employee productivity.**

Logs are regularly reviewed and analyzed for evidence of inappropriate or unusual activity. Inappropriate access is subject to corrective action, up to and including termination.



**See Something? Say Something!**

## **Reporting Suspected HIPAA Violations**

Protecting patient data is a shared responsibility.

Reporting suspicious activity is a crucial component of the organization's overall HIPAA Privacy and Security programs and general cybersecurity defense.

Cybersecurity defense is vitally important because cyberattacks are on the rise:

- Total annual cost to companies worldwide projected to reach \$10.5 trillion in 2025.
- Cyber attacks on the healthcare sector have increased at more than twice the rate of other industries with a 45% rise in attacks since November of 2020.
- 40 million individuals were affected by healthcare cyber attacks in 2023.



## HIPAA's Breach Notification Rule

HIPAA rules define a breach as the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule that compromises PHI security or privacy.

- When PHI is disclosed without consent or used without permission, all covered entities must notify affected individuals of the breach.
- When you are aware of a potential breach, notify:
  - MHS Privacy Officer at 402-354-6863 or [anita.patterson@nmhs.org](mailto:anita.patterson@nmhs.org)
  - Your manager
  - Compliance Hotline at (877)640-0005 (English), (800)216-1288 (Spanish), or [www.lighthouse-services.com/nmhs](http://www.lighthouse-services.com/nmhs)

Scan with your phone:



**See Something? Say Something!**



**See Something? Say Something!**

## **HIPAA's Omnibus Rule**

The Omnibus Rule is a set of modification the Health Insurance Portability and Accountability Act (HIPAA). The Omnibus Rule addresses the following:

- Business Associates and subcontractors are liable for HIPAA compliance and are responsible for their own breaches.
- Patients have an increased right to access and receive electronic copies of their protected health information (PHI). In addition, to have more control over restricting disclosures of their PHI, especially for out-of-pocket payments for health plans.
- Stricter limits are in place for use of PHI for marketing purposes – require patient consent before use their information.
- Health plans are prevented from using genetic information (GINA-Genetic Information Nondiscrimination Act) coverage decisions and require consent for its use.
- Enhances aspects of the Privacy and Security Rule related to research, authorizations, and data security.
- The Office of Civil Rights (OCR) enforces HIPAA and the Omnibus Rule clarifies penalties for violations.



## HIPAA's Enforcement Rule

The Enforcement Rule emphasizes the Office for Civil Rights (OCR) role for responsible enforcing of HIPAA, including the right to investigate complaints involving covered entities and imposing penalties.

- Patients have the right to file complaints with OCR. OCR handles the complaints by conducting investigations and potentially referring investigations to the Department of Justice for criminal violations, if appropriate. Covered entities must cooperate fully with OCR investigations.
- Enforces “minimum necessary” standard, which requires covered entities to disclose or use only the minimum amount of PHI.
- OCR may seek voluntary compliance, corrective actions, or resolution agreements from covered entities to resolve violations.

**See Something? Say Something!**





# Medicare Parts C&D Fraud Waste & Abuse

2025 Annual Safety and Compliance Training (ASCT)

## **Core Learning Objectives of this course:**

When you complete this course, you should correctly:

- Recognize Fraud, Waste and Abuse (FWA) in the Medicare Program
- Identify the major laws and regulations pertaining to Fraud, Waste and Abuse
- Recognize potential consequences and penalties associated with violations
- Identify methods of preventing Fraud, Waste and Abuse
- Identify how to report Fraud, Waste and Abuse
- Recognize how to correct Fraud, Waste and Abuse

## Medicare Part C

Also known as Medicare Advantage (MA), is a health plan choice available to Medicare beneficiaries. Private, Medicare-approved insurance companies run MA programs. These companies arrange for, or directly provide, health care services to the beneficiaries who elect to enroll in an MA plan.

MA plans must cover all services Medicare covers with the exception of hospice care. They provide Part A and Part B benefits and may also include prescription drug coverage and other supplemental benefits.

## Medicare Part D

Known as the Prescription Drug Benefit, provides prescription drug coverage to all beneficiaries enrolled in Part A/Part B who elect to enroll in a Medicare Prescription Drug Plan (PDP) or an MA Prescription Drug (MA-PD) plan.

Medicare approved insurance and other companies provide prescription drug coverage to individuals who live in a plan's service area.

# Effective Compliance Programs



**The Centers for Medicare & Medicaid Services (CMS) requires Sponsors to implement and maintain an effective compliance program for its Medicare Parts C and D plans to:**

Articulate and demonstrate an organization's commitment to legal and ethical conduct;  
Provide guidance on how to handle compliance questions and concerns; and  
Provide guidance on how to identify and report compliance violations.



**An effective compliance program must foster a culture of compliance within an organization and, at a minimum:**

Prevent, detect, and correct non-compliance;  
Be fully implemented and tailored to the organization's unique operations and circumstances;  
Have adequate resources;  
Promote the organization's Code of Conduct; and  
Establish clear lines of communication for reporting non-compliance.

# Ethical Guidelines

As part of the Medicare Program, you must conduct yourself in an ethical and legal manner. **It's about doing the right thing!**

## General Ethical Guidelines:

- Methodist Health System (MHS) will conduct its business in a competent, fair, impartial and efficient manner.
- MHS employees will always demonstrate the highest levels of integrity, truthfulness and honesty in order to uphold personal and corporate reputations and to inspire confidence and trust in their respective actions

The MHS Code of Conduct states our compliance expectations and our principles and values. **Everyone has a responsibility to report violations of the Code of Conduct and suspected non-compliance.**



# Non-Compliance

Non-compliance is conduct that does not conform to the law, Federal health care program requirements, or an organization's ethical and business policies. CMS has identified the following Medicare Parts C and D high risk areas:



- Agent/broker misrepresentation
- Appeals and grievance review (for example, coverage and organization determinations)
- Beneficiary notices
- Conflicts of interest
- Claims processing
- Credentialing and provider networks
- Documentation and Timeliness requirements
- Ethics
- FDRs (First-Tier, Downstream, or Related Entity) oversight and monitoring
- Health Insurance Portability and Accountability Act (HIPAA)
- Marketing and enrollment
- Pharmacy, formulary, and benefit administration
- Quality of care

# Non-Compliance

Failure to follow Medicare Program requirements and CMS guidance can lead to serious consequences including **contract termination, criminal penalties, exclusion from participation in all Federal health care programs, and civil monetary penalties.**

Those who engage in non-compliant behavior may also be subject to any of the following:

- Mandatory training or re-training
- Disciplinary action
- Termination



# Non-Compliance

**In the event that non-compliance is detected, it will be investigated fully and promptly corrected.**

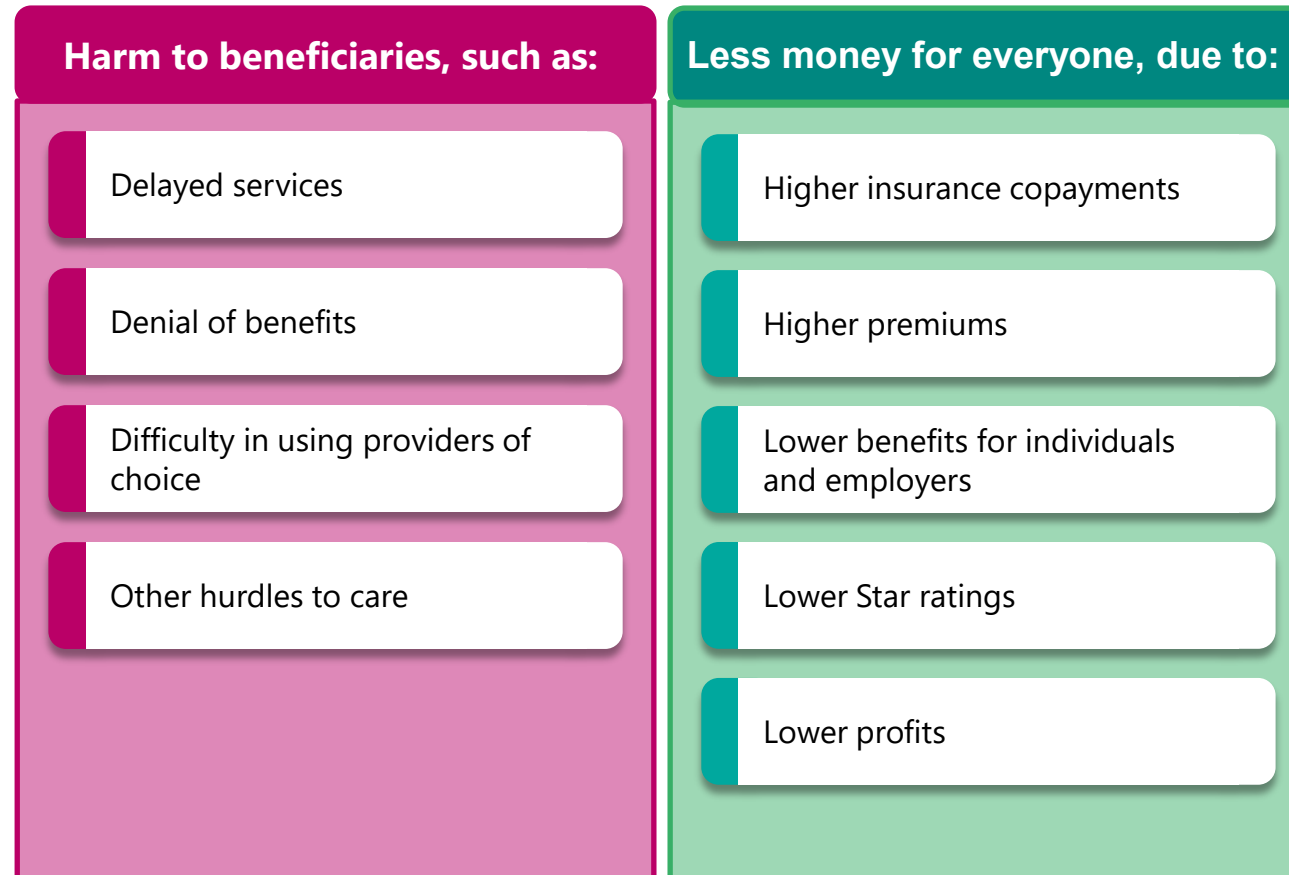
Internal monitoring will continue to ensure:

- No recurrence of the same non-compliance
- Ongoing compliance with CMS requirements
- Efficient and effective internal controls
- Enrollees are protected

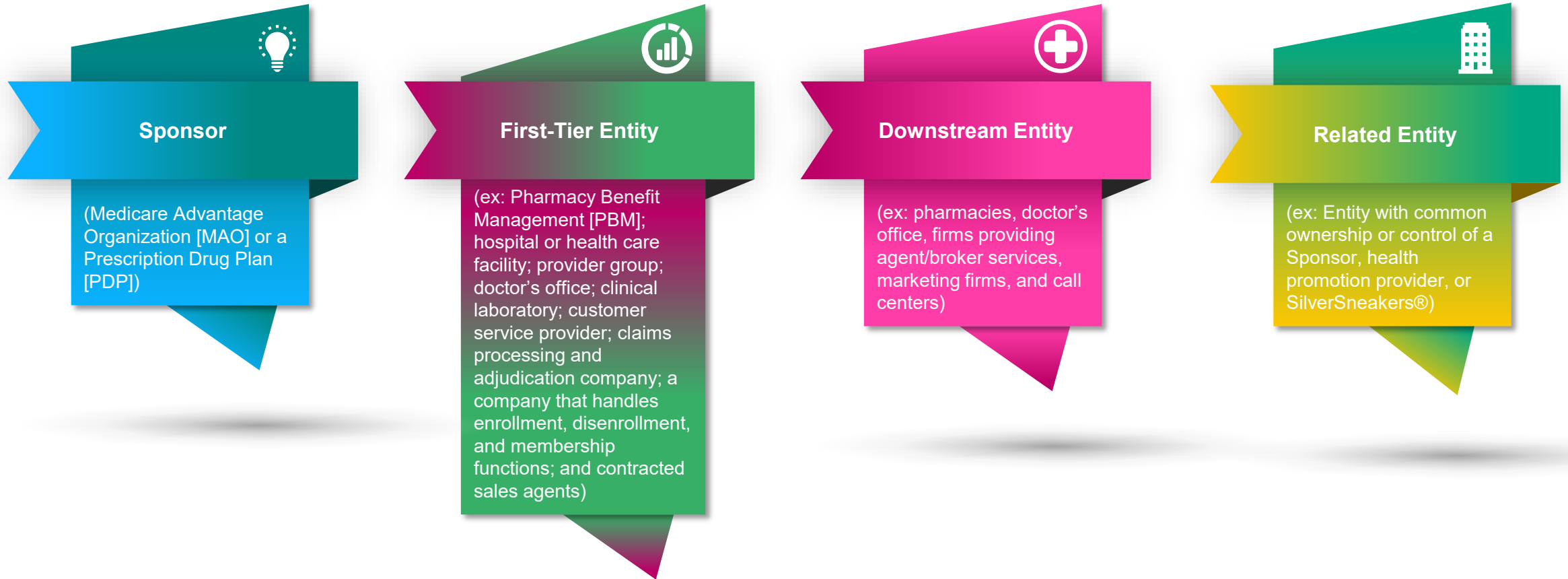




Without programs to prevent, detect, and correct non-compliance, what do we risk?



# As a person who provides health or administrative services to a Medicare Part C or Part D enrollee, you are likely an employee of a:



# Sponsors and Their FDRs (First-Tier, Downstream, or Related Entity)



CMS expects all Sponsors will apply their training requirements and effective lines of communication to their FDRs (First-Tier, Downstream, or Related Entity).

Having effective lines of communication means employees of the Sponsor and the Sponsor's FDRs have several avenues to report compliance concerns.

# Fraud, Waste and Abuse (FWA): Responsibilities

You play a vital part in preventing, detecting, and reporting potential FWA, as well as Medicare non-compliance.



# Preventing Fraud, Waste and Abuse (FWA)



Look for suspicious activity



Conduct yourself in an ethical manner



Ensure accurate and timely data/billing



Ensure you coordinate with other payers



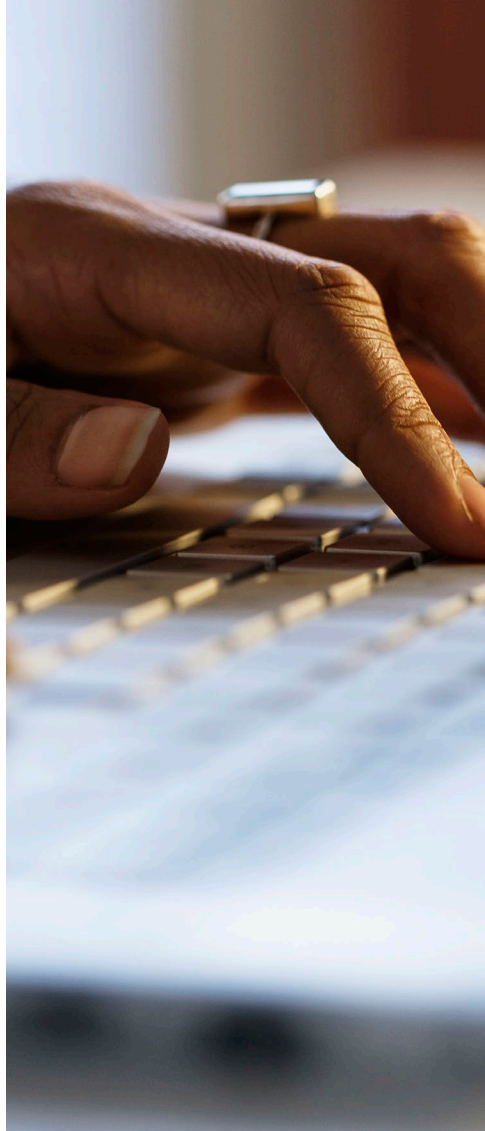
Know FWA policies and procedures, standards of conduct, laws, regulations, and CMS guidance



Verify all received information



Act in accordance with the Code of Conduct



# Compliance Reporting

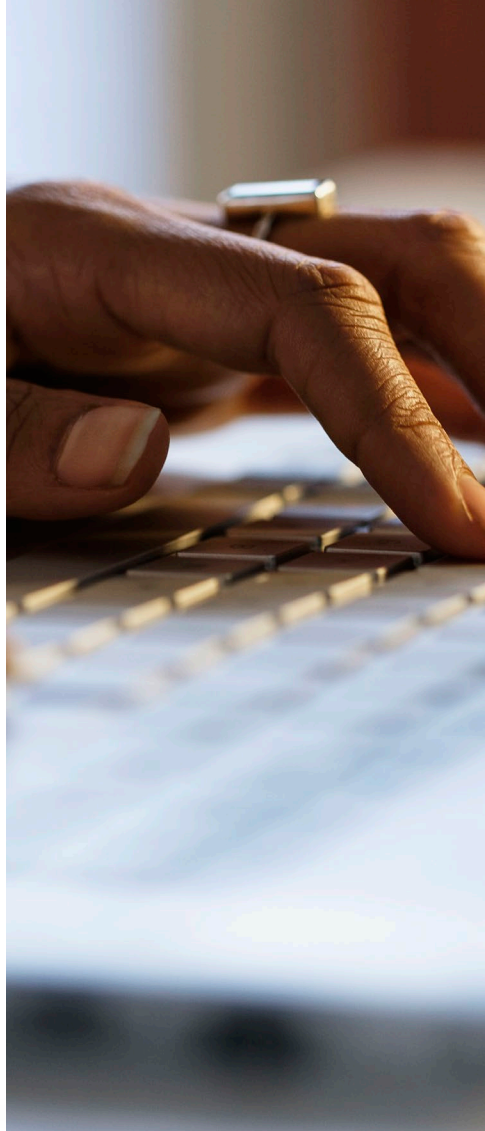
Reporting Compliance Issues, including suspected instances of Fraud, Waste and Abuse:

Employee Center > Departments > Compliance

Call the MHS Compliance Reporting Hotline 24 hours a day:  
877-640-0005 (English) or 800-216-1288 (Spanish)

Contact the VP of Compliance or MHS Chief Compliance Officer directly via email or phone

Contact your supervisor or manager



# Compliance Reporting

Reporting Compliance Issues, including suspected instances of FWA:

All reports to the Compliance Reporting Hotline can be made anonymously.

**No retaliation will be permitted against an employee making such a report.** Employees making reports are encouraged to disclose their identity to allow a full and timely investigation of the concerns, however, anonymous reporting is an option. No report will be refused or treated less seriously because the reporter chooses not to be identified.

# Reporting FWA Outside MHS

If warranted, Sponsors and FDRs must report potentially fraudulent conduct to government authorities, such as the Office of Inspector General, the Department of Justice, or CMS.

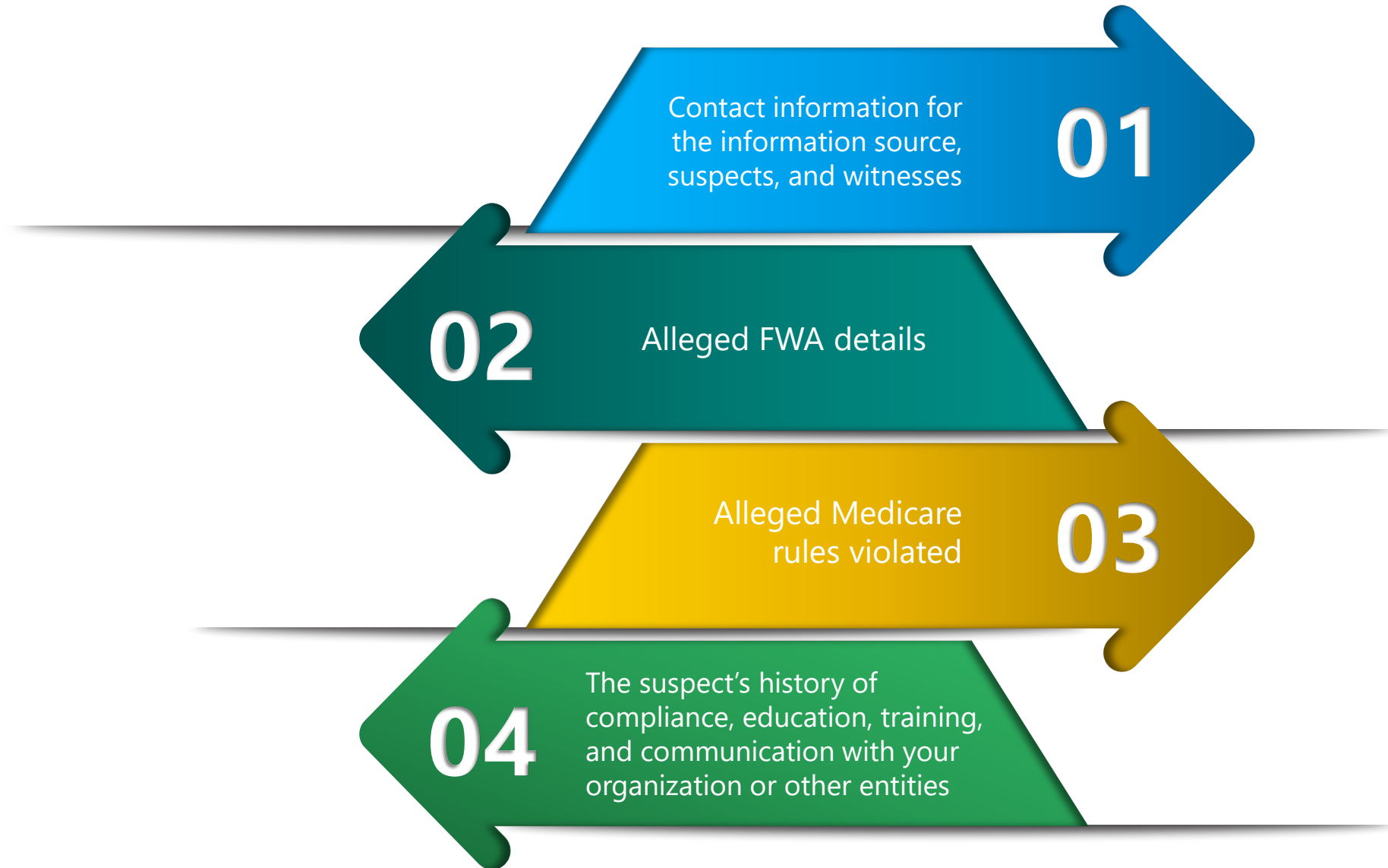
Individuals or entities who wish to voluntarily disclose self-discovered potential fraud to OIG may do so under the Self-Disclosure Protocol (SDP).

Self-disclosure gives providers the opportunity to avoid the costs and disruptions associated with a Government directed investigation and civil or administrative litigation.





# When reporting suspected Fraud, Waste and Abuse include:



# Where to Report FWA:

HHS Office of Inspector General:

- Phone: 1-800-HHS-TIPS (1-800-447-8477)
- TTY 1-800-377-4950
- Fax: 1-800-223-8164
- Email: [HHSTips@oig.hhs.gov](mailto:HHSTips@oig.hhs.gov)
- Online: <https://oig.hhs.gov/fraud/report-fraud/>

Medicare website: <https://www.medicare.gov/basics/reporting-medicare-fraud-and-abuse>



# Corrective Action

**Once fraud, waste, or abuse has been detected, promptly correct it.** Correcting the problem saves the Government money and ensures we are in compliance with CMS requirements.

Compliance will develop a corrective action plan to correct the underlying issue that results in FWA program violations and to prevent future noncompliance. The corrective action plan will be tailored to address the particular FWA, problem, or deficiency identified, it will include concrete steps to follow, and it will include ongoing monitoring to ensure the issue does not reoccur.



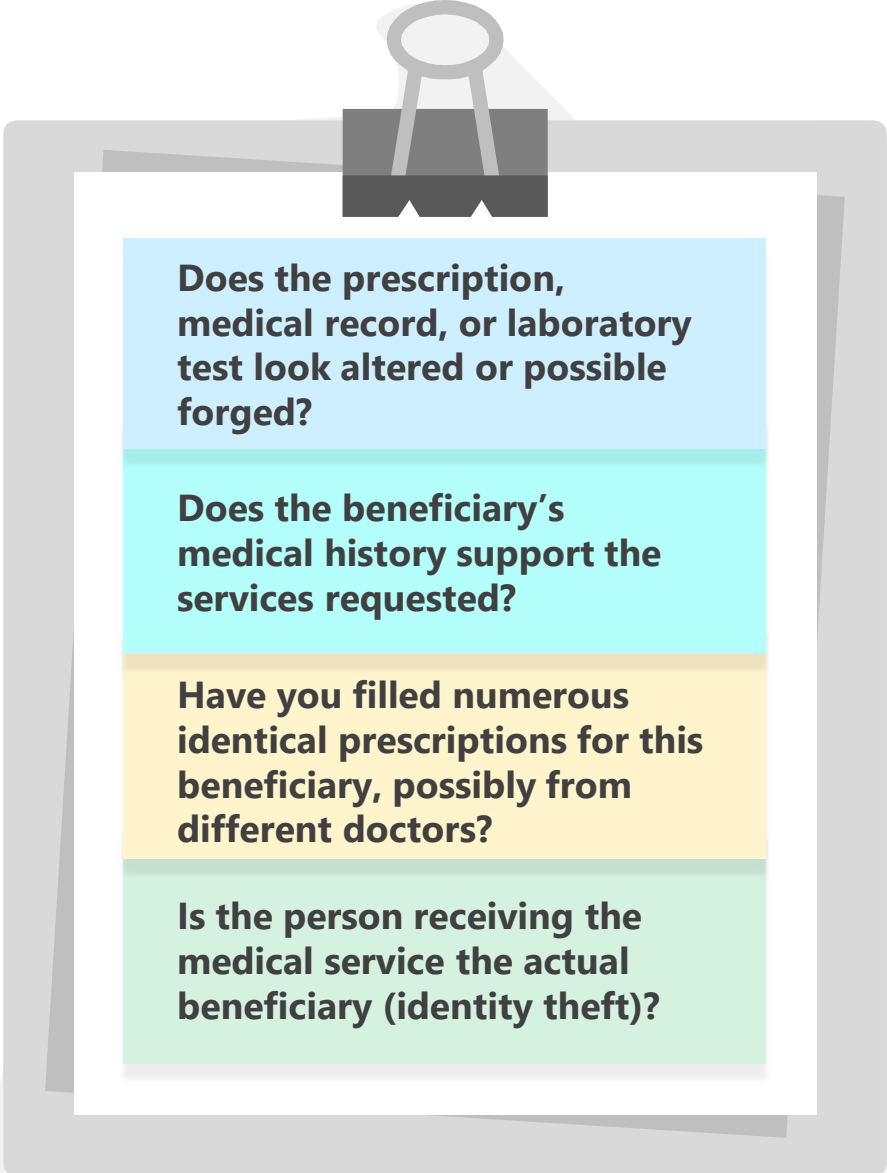
# Corrective Action

## Corrective actions may include:

- Adopting new prepayment edits or document review requirements
- Conducting mandated training
- Providing educational materials
- Revising policies and procedures
- Warning letters, disciplinary action(s)
- Termination



## Potential Issues – Beneficiary

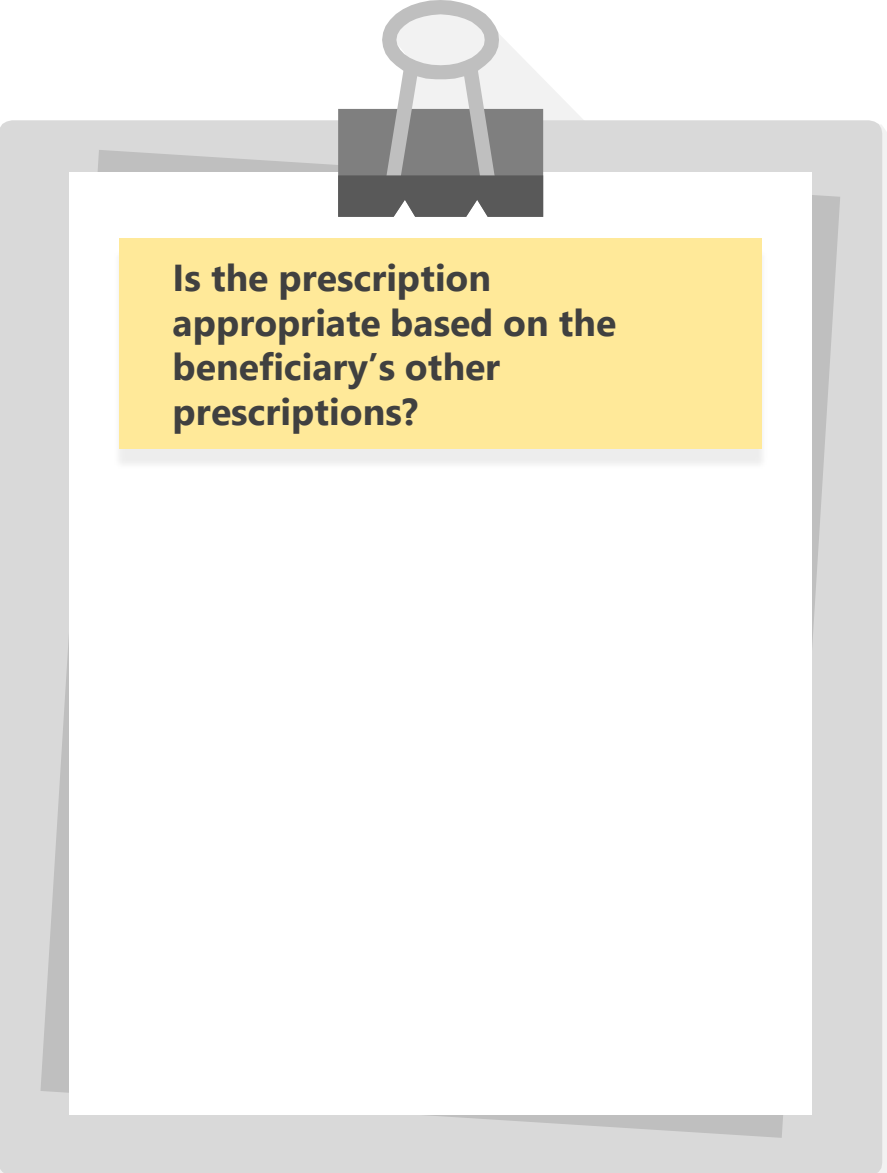


Does the prescription, medical record, or laboratory test look altered or possible forged?

Does the beneficiary's medical history support the services requested?

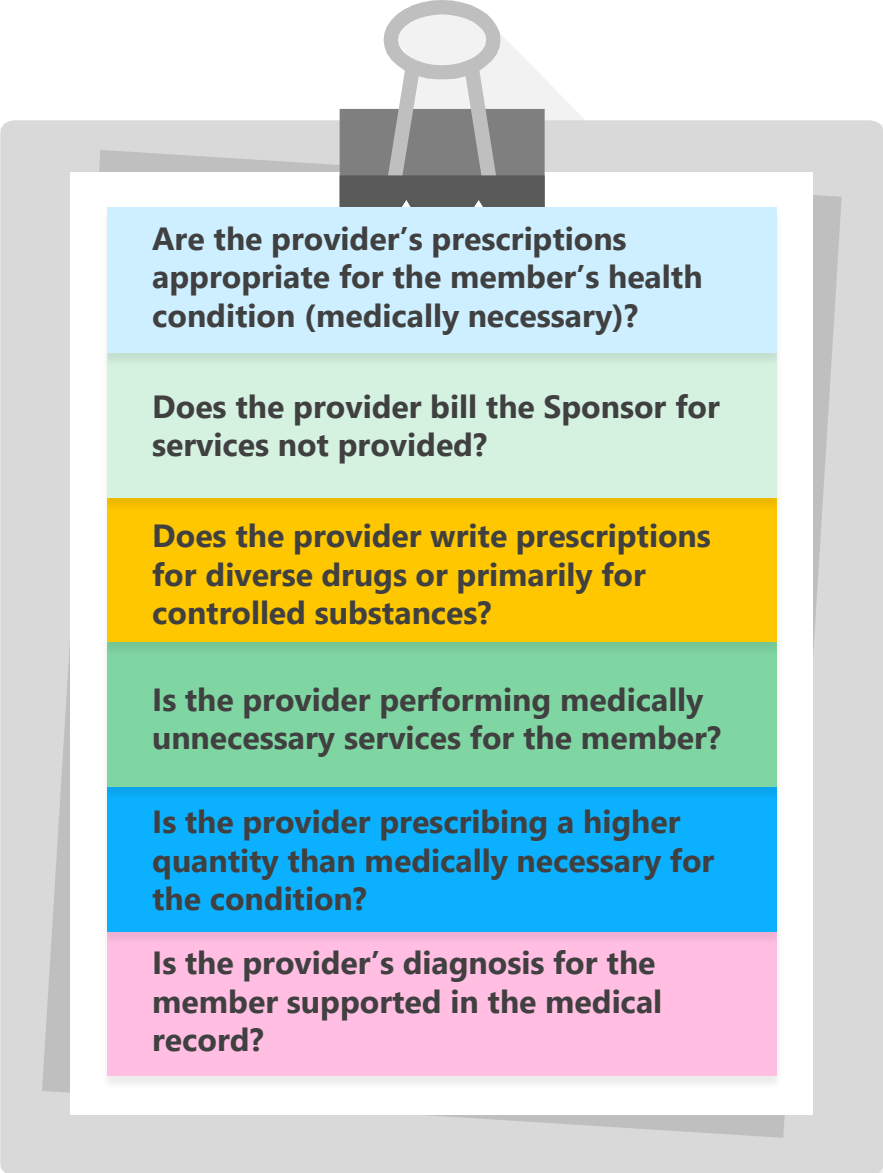
Have you filled numerous identical prescriptions for this beneficiary, possibly from different doctors?

Is the person receiving the medical service the actual beneficiary (identity theft)?



Is the prescription appropriate based on the beneficiary's other prescriptions?

## Potential Issues – Provider



**Are the provider's prescriptions appropriate for the member's health condition (medically necessary)?**

**Does the provider bill the Sponsor 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?**

**Is the provider prescribing a higher quantity than medically necessary for the condition?**

**Is the provider's diagnosis for the member supported in the medical record?**

## Potential Issues – Pharmacy



**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?**

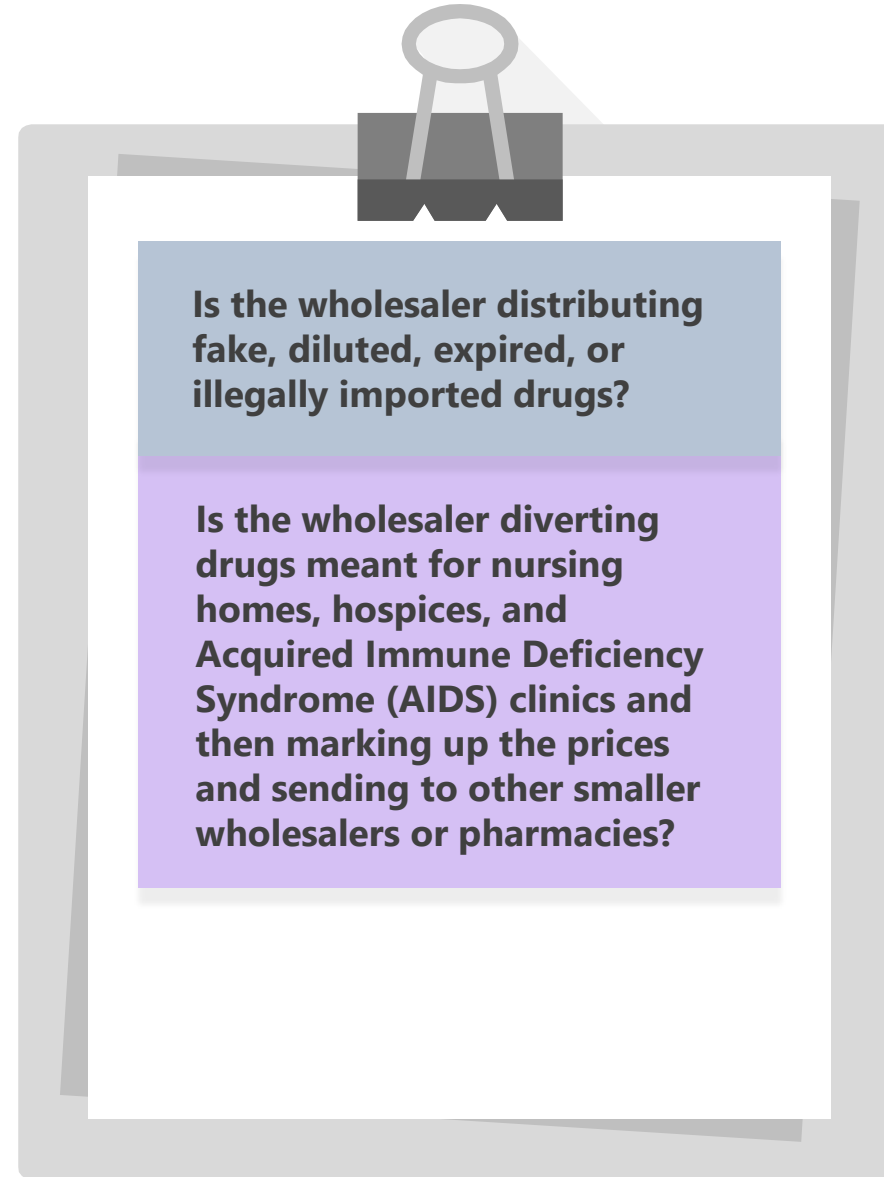
**Are generic drugs provided when the prescription requires that brand drugs be dispensed?**

**Are PBMs being billed for prescriptions that are not filled or picked up?**

**Are proper provisions made if the entire prescriptions cannot be filled (no additional dispensing fees for split prescriptions)?**

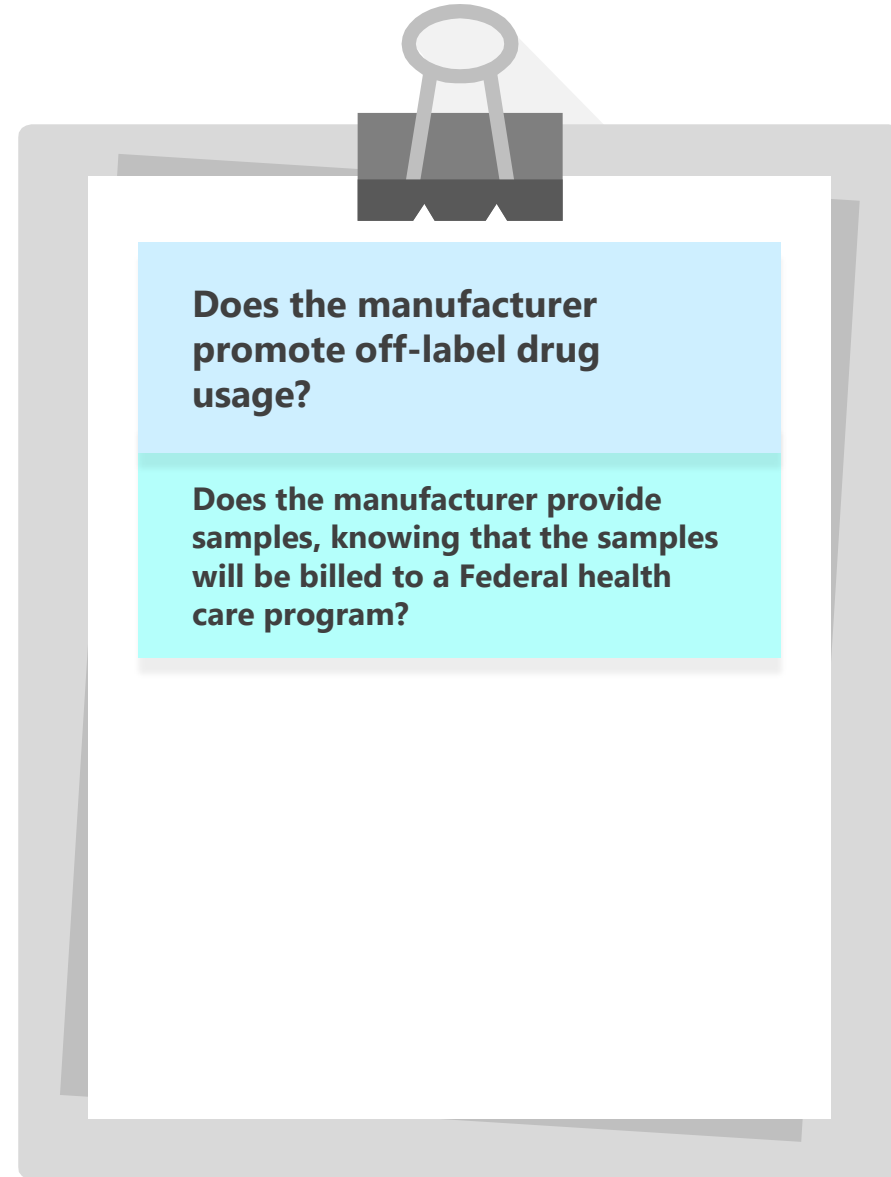
**Do you see prescriptions being altered (changing quantities or Dispense As Written)?**

## Potential Issues – Wholesaler

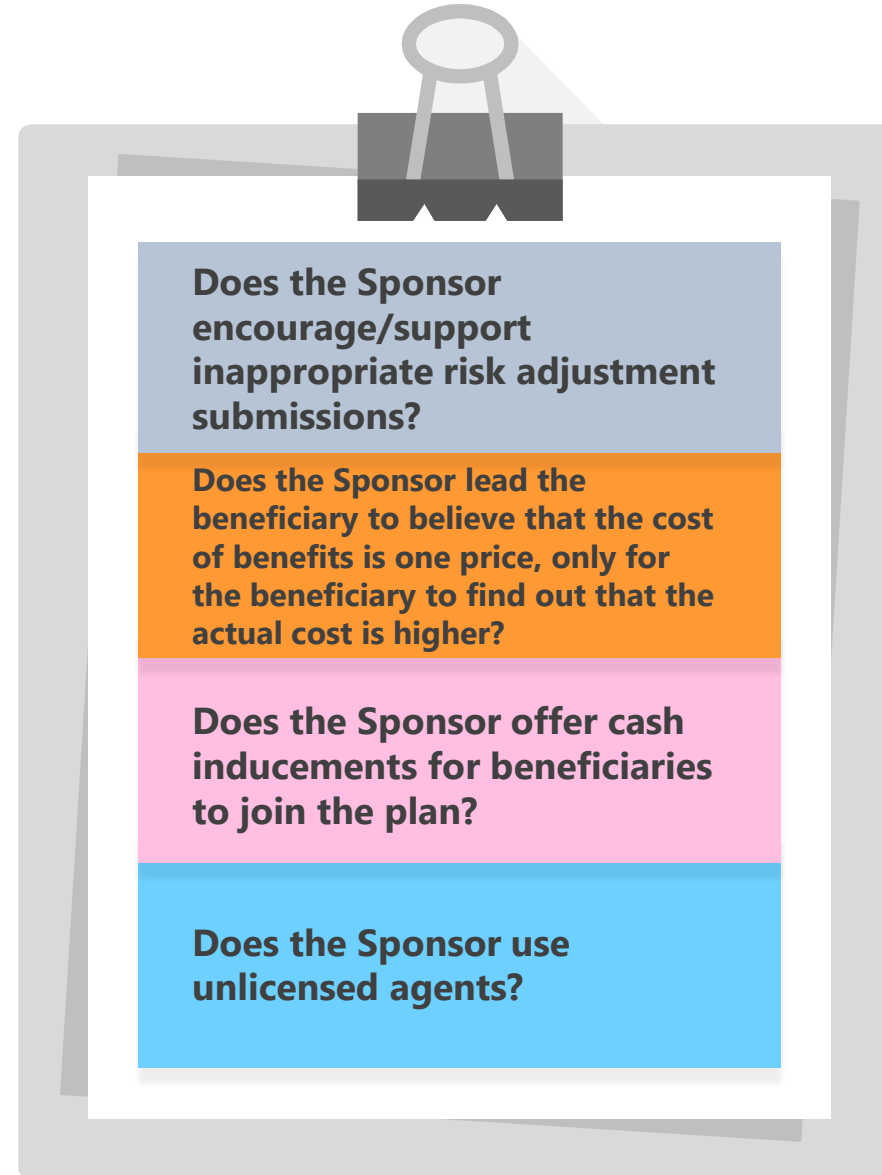




## Potential Issues – Manufacturer



## Potential Issues – Sponsor



# Compliance is Everyone's Responsibility!

As a person providing health or administrative services to Medicare Part C or D enrollees, **you play a vital role in preventing fraud, waste, and abuse (FWA)**. Conduct yourself ethically, stay informed of MHS policies and procedures, and keep an eye out for potential compliance issues.

**Report potential compliance issues.** MHS has mechanisms for reporting potential FWA and other compliance issues. We have options for anonymous reporting, and we will never retaliate against you for making a report in good faith. We will promptly correct identified compliance issues with effective corrective action plans that include ongoing monitoring and auditing.