# Corporate Compliance Program Education



The meaning of care.®

Course 1: Corporate Compliance Plan

Course 2: Code of Conduct

Course 3: HIPAA

Course 4: Medicare Parts C&D

1. General Compliance Training
2. Fraud, Waste, and Abuse

# Corporate Compliance Plan

# Corporate Compliance Plan

## Why Do I Need This Training?

For our Corporate Compliance Program to continue to be successful, every Methodist Health System(MHS) employee and agent needs to understand and take seriously their responsibility to comply with all applicable rules, regulations, policies and procedures and to report any suspected compliance issues.

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

# Objective

Our Corporate Compliance Program is designed to ensure 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: The Corporate Compliance Plan and the Code of Conduct.**

# Your Role in Corporate Compliance

**Everyone has a role in MHS's Corporate Compliance Program!**

You have a substantial impact on MHS's compliance through your role in MHS operations, whether it is patient care, supporting patient care, billing, coding, contracting, or documentation. To help satisfy your role in compliance, you need to know the following:

- The relationship between the Code of Conduct and compliance
- The laws that impact compliance
- The steps necessary to protect patient privacy
- Your role in preventing fraud and abuse

# Corporate Compliance Plan

**The Corporate Compliance Plan consists of seven elements:**

1. Standards, Policies, and Procedures
2. Compliance Program Oversight
3. Training & Education
4. Open Communication and Reporting Systems
5. Monitoring & Auditing
6. Corrective Action Plans
7. Discipline for Noncompliance

**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.**

# Standards, Policies, and 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.

# 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.

# Compliance Program Oversight

**Key Contacts:**

**Shari Flowers**, Vice President of Compliance

**Jen Anderson**, Chief Compliance Officer

**Anita Patterson**, Privacy Officer

**Donna Wellwood-Clawson**, Director Employee Relations

**Michael Kearns**, Director Information Security

# Compliance Program Oversight

## Compliance Contacts

**Shari Flowers**
*VP Compliance*

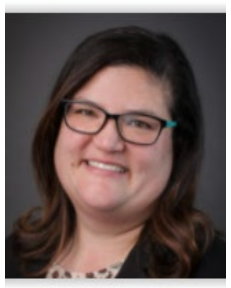
402-354-2163
shari.flowers@nmhs.org

**Jen Anderson**
*Chief Compliance Officer*

402-354-4901
jen.anderson@nmhs.org

**Anita Patterson**
*Privacy Officer*

402-354-6863
anita.patterson@nmhs.org

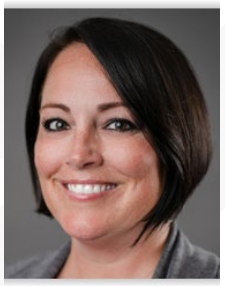


**Jen Woods**
*Compliance Specialist*

402-354-6369
jennifer.woods@nmhs.org

**Joe Tweedt**
*Compliance Specialist*

402-354-6394
joseph.tweedt@nmhs.org



**Stephanie Novak**
*Administrative Assistant*

402-354-2252
stephanie.novak@nmhs.org

# Training and 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.

# 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.**

**MHS Policy:** Compliance Issue Reporting and Non-Retaliation Policy

# Open Communication and Reporting Systems

Everyone is encouraged to contact the Compliance Department for clarification or direction regarding the Code of Conduct. Supervisors may be contacted for assistance with questions about the Code of Conduct.

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

**Reporting Compliance Issues:**

- Contact your supervisor or manager
- Place a direct phone call to the Chief Compliance Officer at 402-354-4901;
- Contact the Compliance Hotline at 877-640-0005 (English) or 800-216-1288 (Spanish);
- Enter a compliance report online at www.lighthouse-services.com/nmhs
- Send a direct email to the Chief Compliance Officer or the VP of Compliance
- Mail questions or concerns to: Chief Compliance Officer, Nebraska Methodist Health System, 825 S. 169th St, Omaha, NE 68118
- Contact the Internal Audit Department

**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.

# Compliance Reporting Hotline

*See Something? Say Something!*

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

Scan with your smart phone camera to easily access the anonymous reporting portal.

LIGHTHOUSE
Obtaining Information, Delivering solutions.

*Compliance Hotline*

- *1-877-640-0005 (English)*
- *1-800-216-1288 (Spanish)*

www.lighthouse-services.com/nmhs

# Monitoring and 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**: Therapy Compliance, Revenue Cycle Compliance, Hospital Compliance, Post-Acute Compliance, Corporate Compliance.

**MHS Policy:** Compliance Auditing And Monitoring

# 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, and system and/or process redesign.

# 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.

**MHS Policy:** Behavioral Improvement/Corrective Action

# 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

# Code of Conduct

# Code of Conduct

The Code of Conduct – also simply called the Code – and related policies serve as the guiding pillars that govern our operations. To be compliant, you need to be familiar with, and follow, the Code and MHS policies.

The Code includes guidance on:

- Shared Responsibility
- Quality of Care and Patient Safety
- Confidentiality and Information Security
- Legal and Regulatory Compliance
- Business and Financial Information
- Workplace Conduct and Employment Practices
- Protecting organizational assets, including our most important asset – YOU!

Honest, ethical, and professional conduct are essential components to our mission: *Improving the health of our communities by the way we care, educate and innovate.* **We hold ourselves and each other mutually accountable for our actions.**

# Corporate Compliance

**Please review the Code of Conduct document linked below. You will be asked to verify that you reviewed this information during the quiz at the end of the course.**


**Code of Conduct**

# Shared Responsibility

**Employee Responsibilities** include:

- Demonstrating professionalism at all times;
- Displaying and promote the highest standards of professional and ethical conduct;
- Acting with the competence, skill, and integrity expected of our professions;
- Behaving with dignity and courtesy toward our patients, clients, coworkers, learners, and others in business-related activities;
- Being honest, fair, reasonable, and objective in our professional relationships.

**Leadership Responsibilities.** Leaders should abide by the Leadership Standards of Behavior, which include:

- **Leading** by motivating, influencing, managing vision and purpose.
- **Standards & Accountability**
- **Planning & Decision Making**
- **Communication**
- **Developing People**
- **Building Relationships**

# Quality of Care and Patient Safety

MHS is committed to assuring a work environment that supports our culture of Safety. It is essential that no one engage in any behavior that may undermine the culture of safety.

Some examples of activities that could jeopardize safety include:

- Failure to report a potential medication error
- Failure to safely dispose of sharps
- Failure to wash your hands between patients
- Failure to report water that has spilled in a hallway
- Failure to use proper lifting techniques or ask for help when lifting

## Patient Rights and Responsibilities

We respect the basic rights of patients to personal dignity and independence of expression, decision-making, and action. Patients shall have the right to receive considerate and respectful care at all times and under all circumstances, with the recognition of personal dignity and respect of religious and cultural beliefs.

**MHS Policy:** Patient Rights and Responsibilities

# Quality of Care and Patient Safety

## Emergency Care

MHS complies with the Emergency Medical Treatment and Labor Act (EMTALA) in providing emergency medical treatment to all MHS hospital patients, regardless of ability to pay or type of payment. MHS hospitals provide a medical screening exam by qualified medical personnel within their capacity to all individuals who come to our hospitals for emergency treatment. MHS does not delay treatment to ask about insurance benefits or financial information. Patients are only transferred to another facility if MHS cannot meet their medical needs and appropriate care is available elsewhere. Patients may only be transferred after they have been stabilized and are formally accepted by another facility. Such patients are transferred by an appropriate mode of transportation after an explanation of the risks and benefits of transfer.

**MHS Policy:** Emergency Medical Treatment and Labor Act EMTALA

## Environment of Care

Each of us is responsible for complying with environmental, health and safety laws and regulations. Observe posted warnings. Report any accidents or injuries to your supervisor immediately. Notify security if a visitor is involved, risk management if a patient is involved, and Employee Health if the injured person is an employee.

# Confidentiality & Information Security

## Patient Confidentiality and Privacy

Confidentiality is the safekeeping of information by individuals who have a need, reason and permission to access such information.

Information about patients, employees, job applicants and MHS itself is confidential. Such information may only be accessed and/or discussed in the line of duty and only with those who have a work related need to know.

Each department will further establish policies of access and/or release of confidential information conducive to their own environment. This information is reviewed with new employees during department/job orientation and annually at Annual Organization Review.

Any access and/or release of confidential information may be cause for corrective action, up to and including termination.

Upon hire, employees are asked to review our written Confidentiality Agreement and sign it.

# Confidentiality & Information Security

## Health Insurance Portability and Accountability Act (HIPAA)

Employees have additional responsibilities under the HIPAA Privacy and Security regulations and MHS policies related to those regulations.

Additional information about HIPAA can be found on the MHS Intranet HIPAA page.

The HIPAA page includes links to all MHS HIPAA Privacy and Security policies, Department Specific Training, Frequently Asked Questions, and HIPAA-related Forms, including the MHS Privacy Notice and Resources.

Consistent with HIPAA, we do not use, disclose or discuss patient-specific information, including patient financial information, with others unless it is necessary to serve the patient or required by law.

# Confidentiality & Information Security

## Social Networking and Technology

MHS employees may not disclose confidential or proprietary information about MHS, its patients, or its employees on social media (including, but not limited to, communications over the Internet, on personal websites or in online forums). We do not take or transmit photographs or records of patients, visitors or staff in the workplace except as permitted by our policies.

Refer to the policy and procedure **Social Networking** for more information. Any questions concerning the appropriate use of social media and technology should be directed, as applicable, to the Privacy Officer, Marketing Department or Information Technology at RESDLI.T.Security@nmhs.org.

# Confidentiality & Information Security

## Information Systems Security

Information systems are those systems where data and/or voice information is processed or stored. Such systems include, but are not limited to: computer systems, removable and non-removable computer storage devices, mobile devices (including smart phones and tablets), voice mail systems and telephones. All Health System employees and agents are bound by the provisions of the HIPAA Security regulations and all MHS policies related to those regulations.

Cellular telephone use is prohibited during work time unless it is necessary in the performance of the employee's job or the employee is on break. The same guidelines apply to sending and viewing text messages. Refer to the policy and procedure **Personal Visits/Telephone Calls/Loitering/Texting/Portable Entertainment Devices** for more information.

In order to protect patient information, medical records, and other confidential information, computers and similar devices are to be used primarily for authorized business purposes only.

All questions regarding IT usage and/or policies should be directed to the MHS Chief Information Security Officer.

# Confidentiality & Information Security

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

# Confidentiality & Information Security

## Identity Theft Prevention

**Appropriate identification of patients is essential**, not only for the protection of patients from identity theft, but also to support the continuum of care for subsequent encounters with the same patient. All employees play a part in preventing patient identity theft by identifying, recording, and reporting any red flags that would suggest a patient's identity is being stolen.

**Red flags** are patterns, practices, or specific activities that indicate the possible existence of identity theft.

If you identify a red flag while interacting with a patient, during treatment, or while working with a patient's medical records, you should make a note of the red flag and report it to your supervisor or the Compliance Department for further investigation and record keeping. **The Compliance department will investigate any red flags and take steps to prevent or mitigate the identity theft.**

**You may face civil or criminal penalties for failure to report red flags that you identify.**

# Confidentiality & Information Security

## Identity Theft Prevention

Red flags that suggest possible identity theft include:

- Identification documents that appear to have been altered or forged or that are not consistent with the appearance of the person presenting the ID
- The name or SSN provided by the person is known by MHS to be the same as another person
- Personal identifying information is provided which is known to be fictitious
- A complaint or question is received from a patient that they received of a bill for another person or for a service that they deny receiving
- A patient or insurance company report that coverage for legitimate MHS stays are being denied because insurance benefits have been depleted, or that a lifetime cap has been reached
- A practitioner's review of medical history with the patient reveals that information in the record is inconsistent with the patient's stated history and may reflect that someone other than the patient has been treated under his or her identity

**MHS Policy:** Suspected or Alleged Identity Theft Prevention Program

# Legal and Regulatory Compliance

## Fraud, Waste, and Abuse

**Fraud** is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care 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 health care benefit program.

**Waste** includes practices that, directly or indirectly, result in unnecessary costs to the Medicare Program, such as overusing services. Waste is generally not considered to be caused by criminally negligent actions but rather by the misuse of resources.

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

# Fraud, Waste, and Abuse: Differences

There are differences among fraud, waste, and abuse. One of the primary differences is *intent* and *knowledge*.

**Fraud requires intent** to obtain payment **and the knowledge** that the actions are wrong.

**Waste and abuse** may involve obtaining an improper payment or creating an unnecessary cost to the Medicare Program, but **does not require the same intent and knowledge**.

# Examples of Fraud, Waste, and Abuse

**Fraud:**

- Any dishonest action conducted with the intent to deceive.
- Forgery or improper alteration of any report and/or its supporting documentation.
- Authorizing or receiving payment for hours not worked.
- Improper write-off of an account of a relative or friend.
- Impropriety in the handling or reporting of money or financial transactions.
- Accepting or seeking anything of material value from vendors or persons providing services/materials to the company [exception: perishable gift less than $50 in value intended for a group of employees, such as pastries, candy or flowers].
- Authorizing or receiving payments for goods not received or services not performed.
- Failing to disclose a potential conflict of interest situation.

**Waste:**

- Ordering excessive laboratory tests
- Not taking advantage of available vendor prompt payment discounts

**Abuse:**

- Unknowingly charging excessively for services or supplies
- Using MHS equipment or supplies to conduct personal business
- Using non-confidential information to get new customer(s) for own outside business

# Legal and Regulatory Compliance

## Physician/Referral Relations

It is the policy of MHS to comply with all applicable Federal and State laws and regulations relating to doing business with potential referral sources, including, without limitation, Stark Law and the Anti-Kickback Statute (AKS).

Generally, the Stark Law and AKS prohibit certain kinds of financial relationships and referral arrangements where federal healthcare programs are involved, though exceptions may apply. The Stark Law is a federal regulation with civil penalties, and the AKS is a criminal statute.

All employees, affiliated physicians, and agents of MHS who know of or suspect issues of non-compliance with the **Anti-Kickback Statute and Stark Law (Physician Referrals)** policy and procedure have an affirmative obligation to report such issues.

**MHS Policy:** Anti-Kickback Statute and Stark Law (Physician Referrals)

# Business and Financial Information

## Record Retention and Destruction

All records are retained (and destroyed) in accordance with all applicable laws, regulations and MHS policies. MHS applies effective and cost efficient management techniques to maintain complete, accurate, and high quality records. Department/Division Directors are separately responsible for development and maintenance of processes for the storage and retention of their respective department's or division's internal records, with the exception of patient medical records. No one may remove or destroy records prior to the specified date without first obtaining permission according to the policy.

**MHS Policy:** Record Retention and Destruction

## Government Inquiries and Investigations

We cooperate with government inquiries as well as internal and external audits and investigations. When receiving non-routine requests, you should consult with the Legal and Compliance Department to ensure that requests are handled properly. We are truthful in what we say. We never alter or destroy records in violation of the law.

# Business and Financial Information

## Accurate Medical Record Documentation

Medical records must be maintained for every person evaluated or treated at any MHS facility. All medical records must be legible, accurate and timely written, and should contain sufficient documentation to support the medical necessity of the services provided.

## Coding and Billing

MHS takes great care to ensure that all coding and billing is accurate and in compliance with all federal and state laws and regulations. MHS prohibits any employee or agent of MHS from submitting any claim for payment that they know is false or fraudulent. Deliberate misstatements to government agencies or other third party payers will expose the employee to potential criminal penalties and disciplinary action.

If you have any questions or wish to report any improper billing or coding, you should contact your supervisor, the Chief Compliance Officer, or the Compliance Hotline.

# Business and Financial Information

## False Claims Act, Reporting, and Whistleblower Protection

The False Claims Act is a federal law that allows a civil lawsuit to be brought against a healthcare provider who does any of the following:

- Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval to the government or a government agency.
- Knowingly conceals or retains an over-payment made by the government or a government agency.
- Knowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim.
- Conspires to defraud the government by getting a false or fraudulent claim allowed or paid.

Nebraska and Iowa each have a state-specific false claims act and additional whistleblower protections.

**And what's at stake?**

The next page highlights a few examples of healthcare organizations that violated laws, rules, and regulations and the extensive penalties they were required to pay to the OIG.

# Examples of Enforcement

**September 9, 2020:** https://www.justice.gov/opa/pr/west-virginia-hospital

Wheeling Hospital Inc., an acute care hospital located in West Virginia, agreed to pay **$50 million** to resolve claims that it violated the False Claims Act by knowingly submitting claims to the Medicare program that resulted from violations of the Physician Self-Referral Law and Anti-Kickback Statute.

**March 31, 2022:** https://www.justice.gov/usao-md/pr/maryland-internal-medicine-physician-agrees-pay

Anuja Kurichh, M.D., an internal medicine physician who operates a medical practice known as PHC Healthcare, LLC in College Park, Maryland, has agreed to pay the United States $555,000 to resolve allegations that she violated the federal False Claims Act by submitting false claims to the United States for medical services that were not performed by her.

**March 31, 2022:** https://www.justice.gov/usao-ma/pr/radeas-llc-agrees-pay-116-million-resolve-allegations-fraudulent-billing

A North Carolina-based clinical laboratory, Radeas LLC, has agreed to pay $11.6 million to resolve allegations that it submitted false claims for payment to Medicare for medically unnecessary urine drug testing.

# Workplace Conduct and Employment Practices

## Just Culture and the Culture of Safety

A Just Culture recognizes that competent professionals make mistakes and will develop unhealthy norms but has zero tolerance for reckless behavior. MHS staff shall recognize risk and hazards, be aware of the behavioral choices we and those around us make, report safety issues and assist others to make better choices when they are engaging in unsafe practices.

## Workplace Violence

OSHA has guidelines for preventing workplace violence in health care settings. Possession of firearms or weapons of any kind on MHS premises is strictly prohibited, except for authorized law enforcement personnel. Any act of violence by an employee, including verbal threats, is grounds for disciplinary action up to and including discharge.

# Workplace Conduct and Employment Practices

## Drug Free Workplace

MHS maintains a drug free workplace (except for physician prescribed medications) and follows the federal drug free workplace standards. Unauthorized use of alcohol or illegal drugs is strictly prohibited. Working while under the influence is a ground for disciplinary action up to and including discharge.

**MHS Policy:** Drug And Alcohol Free Workplace

## Discrimination/Harassment

It is a violation of law to discriminate in any way in the treatment of employees or patients with regard to race, color, religion, sex, national origin, disability or veteran status. All potential discrimination should be immediately reported to Human Resources.

# Workplace Conduct and Employment Practices

## Employment and Screening

All MHS employees, agents and contractors are subject to background checks, including but not limited to checking for whether the individual or entity should be excluded from employment or contracting with MHS based upon:

- Past criminal/illegal activity
- Exclusion list status (e.g. OIG and GSA lists)
- Registration as a sex offender
- A history of abuse, neglect, or mistreatment of adults or children.

**MHS Policy:** Employment Process

**Exclusion lists are databases, maintained by the government,** of individuals that are prohibited from participating in Medicare, Medicaid, or other government programs and contracts. No payment can be made by a federal or state program, either directly or indirectly, for any item or service furnished, ordered, or prescribed by an excluded individual.

**MHS Policy:** Exclusion Screening and Sanctions

# Workplace Conduct and Employment Practices

## Conflict of Interest

Legal issues can arise when employees mix personal interests with job duties, specifically when there is a financial component. **An employee may have a potential conflict of interest if they, or a member of their family, have a financial interest in a company that**:

- Provides goods or services to MHS or an Affiliate
- Purchases goods or services for MHS or an Affiliate
- Engages in any other business or financial transaction with MHS or an Affiliate
- Directly competes with MHS or an Affiliate

## Conflict of Interest

If a potential conflict exists, the Compliance team will assess the business transaction between the parties to ensure it is at fair market value as well as document how that decision was made.

**To avoid any potential issues:**

- Don't participate in activities that conflict with your position at MHS
- Don't accept personal gifts or favors from a patient, physician, contractor, supplier, customer, or anyone who does business with MHS (limited exceptions are detailed in the MHS Gifts and Solicitation with Contractors, Vendors, and Suppliers policy).

Questions regarding potential or actual conflicts of interest should be directed to the employee's supervisor or the Vice President of Compliance.

**MHS Policy:** Conflict of Interest

# HIPAA

# HIPAA

## Why Do I Need This Training?

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.

# Introduction

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.

The HIPAA training will discuss:

- **The Privacy Rule**, which sets national standards for the use and disclosure of PHI;
- **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); and
- **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.

# HIPAA Privacy Rule

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. Record are to be access on a “need to know basis” or within one’s job scope. PHI includes:

- Common identifiers, such as name, address, birth date, and Social Security Number
- Information about past, present, or future physical or mental health or conditions
- Information about the provision of health care to the individual
- 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)

In order to share information on a de-identified basis, the following eighteen (18) specific identifiers must be removed:

1. Names
2. Address
3. Any dates (except years) that are directly related to the individual
4. Telephone number
5. Fax number
6. Email address
7. Social Security number
8. Medical Record number
9. Health Plan beneficiary number
10. Account number
11. Certificate/license number
12. Vehicle identifiers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLS's)
15. Internet protocol (IP) address
16. Biometric identifiers (finger and voice prints
17. Full face photos
18. Any other unique identifying numbers, characteristic or codes

# Confidentiality

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.**
  - 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.

All employees sign a Confidentiality Agreement upon hire.

# Confidentiality

**Protecting Patient Confidentiality Includes**:

- 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.
- 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.

# Confidentiality

**Access to Family Member Medical Records:**

- MHS allows employees to access their own medical record (except psychotherapy notes) and records of their minor, dependent children (generally under the age of 19 in Nebraska and under the age of 18 in Iowa) without an authorization.
- Employees must have a HIPAA compliant “Release of Information” on file in Cerner signed by the relevant family member, if they are not a minor, dependent child, in order to access their medical records.

**Methodist My Care**

Employees are encouraged to sign up for the Methodist My Care patient portal. Methodist My Care is a secure online portal that can help you manage your health information. Please visit methodistmycare.org for additional information.

**MHS Policy:** Accessing Your Own Medical Record

# HIPAA Privacy Rule

The Privacy Rule also gives patients the right to:

- Examine and get a copy of their medical records, including an electronic copy of their electronic medical records.
- Request a correction or amendment if they believe their medical record is inaccurate
- Request an alternative means of communication.
- Opt-Out of the facility directory if an inpatient.
- Request a restriction on the use or disclosure of PHI.
- Receive an Accounting of Disclosures - Patients can request a list of all parties to whom we have released PHI.

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.

# HIPAA Privacy Rule

**The HIPAA Privacy Rule applies 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 the people who work there)
- Health Plans
- 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)
- Any other organization/person that handles PHI

# 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:

- MHS's pledge to keep their information private
- How information about them may be used or disclosed in the process of treatment, collecting payment, and improving healthcare operations
- Options if they feel their rights have been violated

**MHS Policy:** Notice of Privacy Practices

# Social Media Guidelines

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.

***Never*** post confidential information or photos or videos of patients on the internet, even if it does not include a patient's name. Inappropriate posts can seriously damage Methodist Health System's reputation.

***Never*** discuss confidential information in public forums, chat rooms, text messages, or news groups.

***Be cautious*** of identifying yourself as a Methodist employee on social media.

***Do not*** "friend" patients.

***Do not*** use MHS logos/trademarks on your personal posts.

**MHS Policy:** Social Networking Policy

# HIPAA Security Rule

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

1. 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.
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information; and
3. 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. We do this through our IT security personnel, information access management rules and systems, and information security policies and procedures.

The IT security staff develops policies and procedures, monitors systems, tests processes, and trains employees. Our access management controls limit authorized users to only the information they need to perform their job functions.

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

# Administrative Safeguards

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 an Electronic Resource for personal use does not necessarily constitute continuing approval.

**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.**

# Administrative Safeguards

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 report the matter to your supervisor immediately.**

# Administrative Safeguards

**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 you still need 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.

# Administrative Safeguards

Anyone who violates MHS policies faces corrective action based upon the MHS Behavioral Improvement/Corrective Action Guidelines.

**Corrective actions 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.

# Physical Safeguards

Physical safeguards are applied to control facility access 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.
- Controlling workstation access covers many employee responsibilities including:
  - Locking your laptop/computer when not in use;
  - Keeping your password secret;
  - If working from home, securing/encrypting your home network traffic;
  - Being aware of your environment if discussing PHI;
  - Using MHS IT approved software for virtual meetings and communication; and
  - Monitoring for unauthorized or unknown individuals joining meetings where PHI is discussed.

# 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, and is available to, MHS. This information, including emails, may be examined by MHS employees or designees at any time, without notification, and used in any acceptable manner.

# Technical Safeguards

MHS IT systems record and monitor access to our systems, including CERNER, for 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.

# Breach Notification Rule

HIPAA rules define a breach as the acquisition, access, use, or disclosure of 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.
- We must notify authorities of most breaches without reasonable delay and no later than 60 days after discovering the breach. The Breach Notification Rule also requires business associates to notify a covered entity of breaches at or by the business associates.
- Notify your manager and the MHS Privacy Officer at 402-354-6863 when you are aware of a potential breach.

**MHS Policy:** Breach Notification Policy

# Medicare Parts C & D

# Medicare Parts C & D

## Why Do I Need This Training?

As an individual who provides health or administrative services for Medicare enrollees, your every action potentially affects Medicare enrollees, the Medicare Program, or the Medicare Trust Fund. **Every year, billions of dollars are improperly spent because of Fraud, Waste, and Abuse. It affects everyone – including you.**

This training fosters our culture of compliance, and it helps you detect, correct, and prevent fraud, waste, and abuse. **You are part of the solution.**

# Medicare Parts C & D

**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**, the Prescription Drug Benefit, provides prescription drug coverage to all beneficiaries enrolled in Part A and/or 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 f**oster 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:

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

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
- FDR 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

**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

# Non-Compliance

Without programs to prevent, detect, and correct non-compliance, we all risk the following:

**Harm to beneficiaries, such as:**

- Delayed services
- Denial of benefits
- Difficulty in using providers of choice
- Other hurdles to care

**Less money for everyone, due to:**

- Higher insurance copayments
- Higher premiums
- Lower benefits for individuals and employers
- Lower Star ratings
- Lower profits

# Fraud, Waste, and Abuse

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:

- **Sponsor** (Medicare Advantage Organization [MAO] or a Prescription Drug Plan [PDP])
- **First-Tier Entity** (ex: Pharmacy Benefit Management [PBM]; hospital or health care facility; provider group; doctor's office; clinical laboratory; customer service provider; claims processing and adjudication company; a company that handles enrollment, disenrollment, and membership functions; and contracted sales agents)
- **Downstream Entity** (ex: pharmacies, doctor's office, firms providing agent/broker services, marketing firms, and call centers)
- **Related Entity** (ex: Entity with common ownership or control of a Sponsor, health promotion provider, or SilverSneakers®)

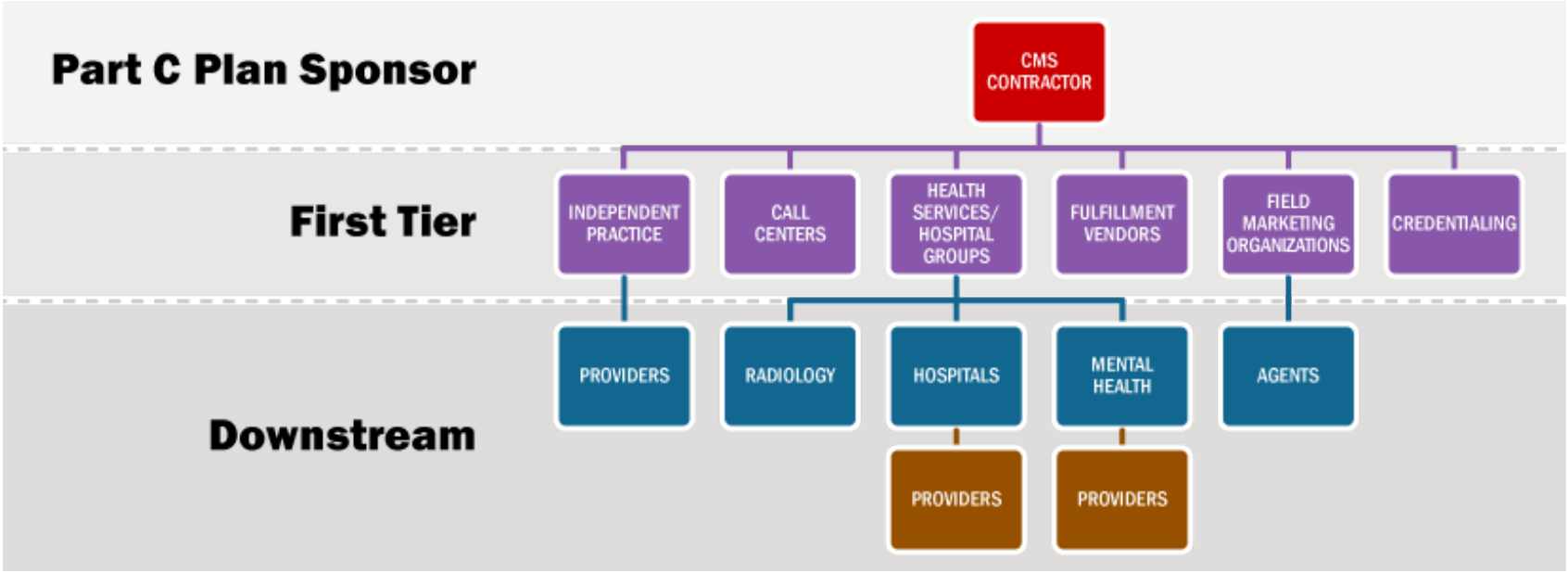
# Sponsors and Their FDRs

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

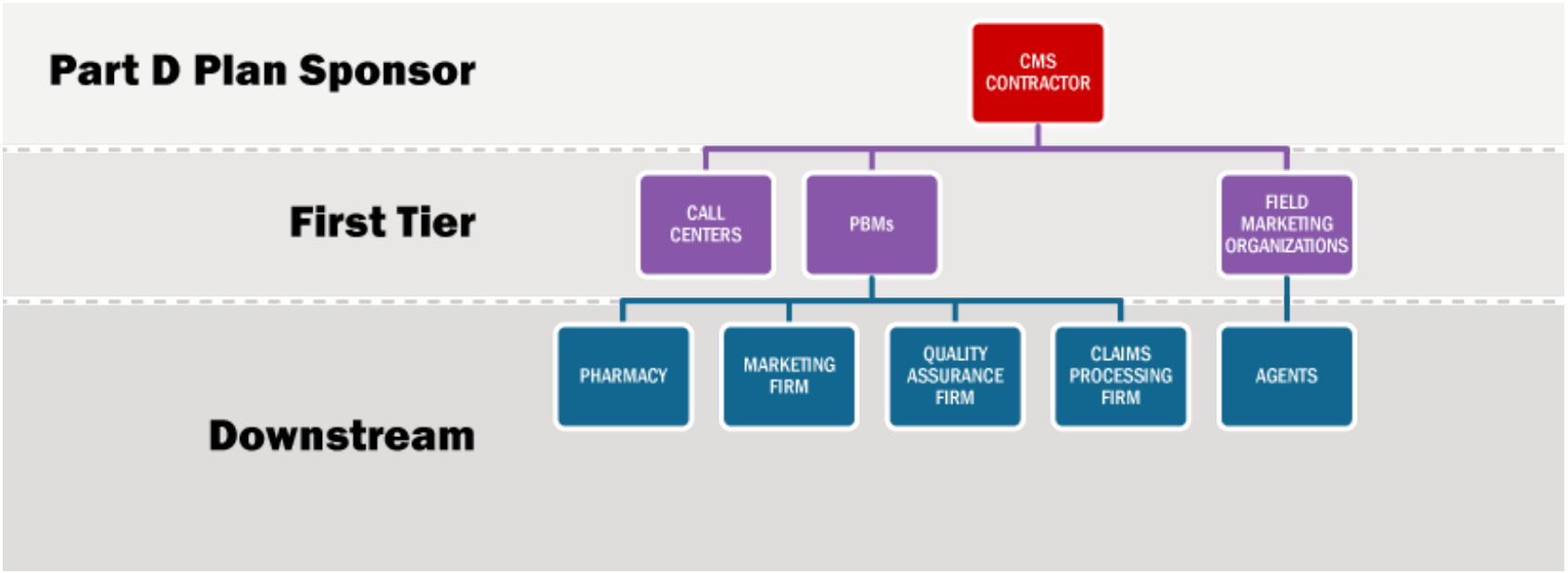
Having effective lines of communication means employees of the Sponsor and the Sponsor's FDRs **have several avenues to report compliance concerns**.

To review your options for reporting visit the mhsintranet > Resources > Compliance.

# Fraud, Waste, and Abuse



# Fraud, Waste, and Abuse



# FWA: Responsibilities

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

**FIRST**, you must comply with all applicable statutory, regulatory, and other Medicare Part C or Part D requirements, including adopting and using an effective compliance program.

**SECOND**, you have a duty to the Medicare Program to report any compliance concerns, and suspected or actual violations of which you may be aware.

**THIRD**, you have a duty to follow the MHS Code of Conduct that articulates your and the organization's commitment to standards of conduct and ethical rules of behavior.

# Preventing 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 FWA:

1. Use the **MHS Compliance Reporting Link** on the mhsintranet (Resources tab > Compliance)
2. Call the **MHS Compliance Reporting Hotline** 24 hours a day
    - **877-640-0005 (English) or 800-216-1288 (Spanish)**
3. **Contact the VP of Compliance or MHS Chief Compliance Officer** directly via email or phone
4. Contact your supervisor or manager

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.

# Reporting FWA Outside MHS

When reporting suspected FWA, include:

- Contact information for the information source, suspects, and witnesses
- Alleged FWA details
- Alleged Medicare rules violated
- The suspect's history of compliance, education, training, and communication with your organization or other entities

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
  - Online: Forms.OIG.hhs.gov/hotlineoperations/index.aspx
- Medicare beneficiary website: Medicare.gov/forms-help-resources/help-fight-medicare-fraud/how-report-medicare-fraud

# 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.

We 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

# Key Indicators of FWA

## 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?

# Key Indicators of FWA

**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?

# Key Indicators of FWA

## 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)?

# Key Indicators of FWA

## Potential Issues – Wholesaler

- Is the wholesaler distributing fake, diluted, expired, or illegally imported drugs?
- Is the wholesaler diverting drugs meant for nursing homes, hospices, and Acquired Immune Deficiency Syndrome (AIDS) clinics and then marking up the prices and sending to other smaller wholesalers or pharmacies?

# Key Indicators of FWA

**Potential Issues – Manufacturer**

- Does the manufacturer promote off-label drug usage?
- Does the manufacturer provide samples, knowing that the samples will be billed to a Federal health care program?

# Key Indicators of FWA

## Potential Issues – Sponsor

- Does the Sponsor encourage/support inappropriate risk adjustment submissions?
- Does the Sponsor lead the beneficiary to believe that the cost of benefits is one price, only for the beneficiary to find out that the actual cost is higher?
- Does the Sponsor offer cash inducements for beneficiaries to join the plan?
- Does the Sponsor use unlicensed agents?

# Course Summary

**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.

**Save or print the resources found in the upper right corner for future use >**