MemorialCare is committed to carrying out its mission and attaining its vision in accordance with the values and ethical principles it has established to govern itself. There has long been a MemorialCare tradition of pursuing excellence. This consistent pursuit and adherence to the values that guide the organization contribute greatly to the MemorialCare operational work environment that encourages good decision-making and promotes a healthy culture of compliance with laws, regulations, best practice standards and program requirements of federal, state and private health plans.

This training module ensures that employees are aware of key MemorialCare policies and government regulations while assisting them in making ethical and compliant choices.
Compliance Training Overview

- MemorialCare Compliance Program
- MHS Code of Conduct with Emphasis on Fraud & Abuse
- HIPAA Privacy & Security Update
- CMS Medicare Part C&D Compliance Training
MemorialCare has a compliance program in place to bring awareness to its workforce in regard to following regulations, policies, procedures and the MHS Code of Conduct. This makes compliance the responsibility of everyone.
Key Elements of MemorialCare’s Compliance Program

- Effective Compliance Program
- Oversight
- Enforcing Disciplinary Standards
- Risk Assessment
- Policies & Procedures
- Training & Education
- Effective Lines of Communication
- Auditing & Monitoring
- Responding to Deficiencies
MemorialCare Compliance Oversight Structure

**Highest Levels of Authority**
- MHS Board of Directors (Approves Compliance Plan)
- Subsidiary Board of Directors

**Campus & System Executive Leadership**
- Support Compliance Plan & Objectives
- Receive Compliance Reports
- Work collaboratively with the MHS CCO to implement compliance initiatives
- CEO’s are ultimately responsible for compliance matters of their entity

**MHS Chief Compliance Officer**

**MHS Compliance Committee**
- High Level Oversight/Work Group
- Establishes and Monitors Compliance Program Activities
- Develops/Approves Organizational Compliance Policies

**MHS Office of the General Counsel**
- Advises & Represents the Organization on Legal Matters
- Educates/Informs Organization on/of Pertinent Laws, Regs, & Standards

**Others With Oversight Role**
- Department Managers
- Focused Compliance Plan Teams

**Twice Yearly Reports**
Compliance Team

Chris Finch
VP Chief Compliance & Audit Officer
Cfinch@memorialcare.org
714-377-3218

Amanda Tillitt
Manager of Compliance
Atillitt@memorialcare.org
714-377-3208

Dyanna Cisneros
Compliance Coordinator
Dcisneros@memorialcare.org
714-377-3205

Tina Cordell
Compliance & Appeals Coordinator
Tcordell@memorialcare.org
714-377-3235

Josh Spreeman
Compliance Data Coordinator
Jspreeman@memorialcare.org
714-377-3234
Key Compliance Policies & Procedures

- Code of Conduct (MHS P&P 303)
- Responsible Use of Technology (MHS P&P 126)
- Conflict of Interest (MHS P&P 112)
Code of Conduct
This section is meant to provide you with an overview of the Memorial Health Services (MHS) Code of Conduct. This training helps MHS ensure that you and all members of its workforce are aware of your personal responsibility and duty to obey related laws and provide you the resources if you believe a law may have been violated. If you would like to read the entire Code of Conduct, please visit the MHS Compliance and Business Ethics website after the training.
Objectives

By the end of this section you should be able to:

• Know the principles of the Code of Conduct
• Identify and describe what a “False Claim” is
• Understand rights of employees to be protected from retaliation if they report fraud
• Identify and describe conflict of interest
• Identify where to go for help if you suspect there is a violation of the Code of Conduct
Legal Compliance

MemorialCare intends that all its activities will be in compliance with applicable laws and regulatory standards. Below is a summary of some of the important legal and regulatory standards that govern healthcare providers, including MemorialCare. This summary is intended to assist you in compliance, but is neither exclusive nor complete. MemorialCare employees and members of MemorialCare medical staffs are required to comply with all applicable laws, whether or not specifically addressed in the summary below. Questions regarding the existence of, interpretation or application of legal requirements or regulatory standards should be directed to your supervisor, the Compliance Department, or the Legal Department.
Legal Compliance: Fraud and Abuse

MemorialCare expects its workforce never engage in conduct which may violate federal and state fraud and abuse/anti-kickback laws. These laws prohibit:

1. Direct, indirect or disguised payments or other incentives in exchange for the referral of patients.

2. Submission of false, fraudulent or misleading claims/reports to any government entity or third party payer. Only services actually provided and accurately and fully documented in patients’ medical records may be billed, and MemorialCare will comply with all applicable program or contractual requirements.

3. Making false, unfair, or dishonest representations; and releasing false, unfair, or dishonest advertising.
Legal Compliance: False Claims Act

The federal False Claims Act (31 USC § 3729-33) helps the federal government combat fraud and recover losses resulting from fraud in Federal programs such as Medicare and Medicaid. Violations of the False Claims Act can include knowingly: (1) submitting a false claim for payment, (2) making or using a false record or statement to obtain payment for a false claim, (3) conspiring to make a false claim or get one paid, or (4) making or using a false record to avoid payments owed to the U.S. Government. “Knowingly” means that a person: (1) has actual knowledge that the information is false; (2) acts in deliberate ignorance of the truth or falsity of the information; or (3) acts in reckless disregard of the truth or falsity of the information.

California False Claims Act
California has its own False Claims Act (Cal. Gov’t Code §§ 12650-12655) is the California version of the federal False Claims act, which applies to programs funded by the State.
Examples of potential false claims include:
• Billing for services that were not provided
• Billing for services that were provided, but were not medically necessary
• Submitting inaccurate or misleading information about the type of services provided
• Making false statements to obtain payment for products or services

Making false statements to obtain payment for products or services

The False Claims Act also allows people with information concerning fraud involving government programs to file a lawsuit on behalf of the government. If the lawsuit is successful, the individual may be entitled to receive a part of the recoveries received by the government. The False Claims Act also protects individuals who report alleged fraud in good faith from retaliation (see “Whistleblower Protections” below). Penalties for violating the federal False Claims Act are significant. Financial penalties for submitting a false claim can total as much as three times the amount of the claims, plus fines of $5,500 - $11,000 per claim.
Legal Compliance: Whistleblower Protection

The federal and California False Claim Acts protect employees from retaliation if they, in good faith, report alleged fraud. Employees cannot be fired, demoted, threatened or harassed as a result of alleging a False Claims Act violation or filing a False Claims Act lawsuit. Penalties for such retaliation can include double lost wages plus interest, reinstatement, and compensation for their costs. Please contact the MemorialCare Chief Compliance Officer at (714) 377-3218 or the Ethics Hotline (888) 933-9044 if you have any questions regarding the federal or California False Claims Acts. We encourage you to report any suspected violations of these, or any other laws described in the Code of Conduct.
Workplace Environment Standards

Professional Conduct
MemorialCare employees and other representatives are expected to project professional, polite and friendly behavior toward MemorialCare patients, clients and vendors.

Honest Communication
MemorialCare requires honesty from people in the performance of their responsibilities and in communication with our lawyers, auditors, and others.

Unfair and Unlawful Treatment
MemorialCare believes that the fair and equitable treatment of employees, patients and other persons is critical to fulfilling its vision and goals. MemorialCare is committed to providing a work environment free of unlawful discrimination, and harassment and retaliation. MemorialCare does not permit or tolerate unlawful discrimination, harassment or retaliation and maintains policies to reinforce its commitment to compliance with applicable laws. Every employee is expected to adhere to a standard of conduct that is respectful of all persons within the work environment and to follow all applicable laws and MemorialCare policies. MemorialCare is also committed to reasonably accommodating employees because of medical reasons or religious beliefs, observances or practices in accordance with applicable law and MemorialCare policy.
Workplace Environment Standards

Unlawful Retaliation
MemorialCare is committed to providing a work environment free of unlawful retaliation. MemorialCare does not permit nor tolerate unlawful retaliation and maintains policies to reinforce its commitment to compliance with applicable laws. Every employee is expected to adhere to a standard of conduct that is respectful of all persons within the work environment and to follow all applicable laws and MemorialCare policies. Any employee who feels that applicable laws or MemorialCare policies have been violated must report alleged violations in accordance with such policies or with this Code of Conduct. MemorialCare will not retaliate against any employee for making a report or filing a complaint.

Accurate Recording of Information
Employees are responsible for making sure that accurate information is recorded on all MemorialCare documents such as their employment applications, time cards, medical records, and benefit forms.
Integrity & Compliance: Confidentiality

**Patient Information**
Workforce members will not speak about any personal or private information concerning patients unless supported by true business or patient care purposes.

**Proprietary Information**
Proprietary information such as trade secrets, ways of doing things, or processes belonging to MHS will not, without prior approval by the workforce member’s supervisor, be shared, told to people, or discussed outside of MHS. This applies to current as well as former workforce members.

**Personnel Actions/Decisions**
Salary, benefit and other personal information relating to workforce members will be treated as confidential. Personnel files, payroll information, disciplinary matters and similar information will be maintained in a manner designed to make sure of confidentiality in accordance with applicable laws.
Conflicts of Interest

Conflicts of interest occur when your personal interests or activities influence or appear to influence your actions and decisions. They also occur when you allow another interest to be more important to your decisions than the interests of MemorialCare and its patients, members, students, residents, and customers. When representing the interest of MemorialCare, it is important to avoid activities and relationships that may impair independent judgment and unbiased decision-making.
Conflicts of Interest

While not all-inclusive, the following is a guide to the types of activities which might cause conflicts of interest.

a) Ownership in, providing consulting services to, or employment by any outside concern which does business with or competes with MemorialCare.
b) Conducting non-MemorialCare business with any MemorialCare vendor or service provider.
c) Representing MemorialCare in a transaction in which you or a member of your family or household has a financial interest.
d) Using confidential information of MemorialCare for personal gain or advantage.
e) Entering into a transaction or activity where personal interests are advanced at MemorialCare’ expense.
f) Entering into a transaction that may cause loss or embarrassment to MemorialCare.
g) Entering into outside activities or employment that interferes with job performance or conflicts with scheduled working hours for MemorialCare.
Conflicts of Interest

**No Providing Services to Competitors/Vendors**
No exempt employee may perform work or render services for any competitor of MemorialCare or for any organization with which MemorialCare does business or without the written approval from the VP of Human Resources, nor may any such employee permit his/her name to be used in any fashion (e.g., an endorsement) that would tend to indicate a business connection with a competitor or vendor of MemorialCare.

A non-exempt employee may work for a competitor in a non-management position, provided such employment does not result in the disclosure of proprietary information or otherwise interfere with his/her employment by MemorialCare.

**Participation on Boards of Directors/Trustees**

a) An exempt employee must notify his supervisor and obtain written approval from the VP of Human Resources prior to serving as a member of the Board of Directors/Trustees of any organization whose interests may conflict with those of MemorialCare.

b) All fees/compensation (other than reimbursement for expenses arising from Board participation) that are received for Board services provided during normal work time shall be paid directly to MemorialCare.

c) An employee must disclose all Board of Directors/Trustees activities in the annual Conflict of Interest disclosure statement.

d) MemorialCare retains the right to prohibit membership on any Board of Directors/Trustees where such membership might conflict with the best interest of MemorialCare.
Conflicts of Interest

Annual Questionnaire
Every employee upon employment, and each director, officer and key employees (persons with responsibilities of a Vice President or higher) of MemorialCare annually, will be required to complete a Conflict of Interest Questionnaire. In addition, employees and other individuals who are in a position to influence selection of vendors or other purchasing decisions may also be asked to complete conflict of interest questionnaires from time to time.

Business Development and Acknowledgment
Subject to your supervisor’s approval, you may offer gifts, entertainment and meals of nominal value to MemorialCare customers, current and prospective business partners and others when such activities have a legitimate business purpose, are reasonable, and are consistent with all applicable laws. For example, you may invite a vendor or consultant to lunch to discuss a new project or celebrate a project completed successfully.
Gifts & Entertainment

Accepting gifts and offers of entertainment creates a risk that our judgment and decisions can be influenced. In some cases, acceptance of gifts and entertainment may be considered a violation of federal and/or state laws. Any gift, regardless of value, may not be accepted if the gift is given to you in an attempt to influence your behavior or decision-making on behalf of MemorialCare.
Gifts & Entertainment

Below are the standards all MemorialCare employees and others (e.g., contracted medical directors) representing MemorialCare are expected to follow:

a) Do not accept or request any gifts, cash or cash equivalents (such as gift cards) or offers of entertainment from any vendor (anyone MemorialCare does business with/where product or services are exchanged), patient, doctor or employee, or any other source that could influence your decisions on behalf of MemorialCare or create the impression of influence.

b) You may accept non-cash gifts of nominal value from time to time, such as consumables (a fruit basket or box of candy) that can be shared with others in your department, or small logo items of insignificant value (such as pens or mugs), but use good judgment to avoid the impression that your judgement or decision making has been compromised or influenced.

c) Except when other non-MemorialCare clients/potential clients are also in attendance, you may not accept meals at a vendor’s expense. Other than as part of a local, regional or national professional meeting or conference, you may not accept entertainment at a vendor’s expense.

d) Attendance at local, vendor-sponsored meetings is permitted. Attendance, at vendor expense, at out-of-town meetings is not permitted, except that expenses may be reimbursed if you are an official speaker or presenter at the meeting.

More specific guidance is provided in the MemorialCare Gifts Policy #225.

Violations of these standards and/or the Gifts policy will be subject to discipline, and at a minimum, suspension from all participation in the selection of vendors for MemorialCare for at least one year.
MHS’ Ethics and Compliance Hotline System

The Corporate Compliance Department is available to answer questions you may have regarding the Code of Conduct. Additionally, MemorialCare has voluntarily put in place an Ethics Hotline for reporting suspected violations of this Code of Conduct, legal requirements, regulatory standards, or policies and procedures by others within MemorialCare without fear of retaliation. Although MemorialCare encourages you to discuss your concerns with your supervisor, our Ethics Hotline allows you to report (anonymously if you so choose) any event or situation you feel is unethical, illegal or irresponsible.

TELEPHONE: (888) 933-9044

E-MAIL: EthicsHotline@memorialcare.org

Please note callers can remain anonymous.
HIPAA Privacy & Security Update
The **Health Insurance Portability and Accountability Act** (HIPAA) is often referenced when discussing patient privacy. HIPAA consists of:

- Privacy Rules
- Security Rules
- Breach Notification Rules
- Administrative Simplification Rules
- Enforcement Rules
- HITECH
- Final Omnibus Rule

However, California privacy rules have stricter reporting and notification requirements than HIPAA.
MemorialCare is required to:

- Prevent unlawful or unauthorized access, use or disclosure of patient medical information
- Report confirmed privacy & security breaches to the California Department of Public Health, The Office for Civil Rights and to the Patient
- Failure to report results in fines/penalties of $100 per day up to a maximum of $250,000

In addition:

- Patients can bring a private cause of action by filing a lawsuit as a result of privacy/security incidents
- California OHII will contact licensing boards, such as the California Medical Board and the Board of Registered Nursing related to violations.

Protect yourself and our patients; think before you access!
Cal. Health & Safety Code §1280.15(b)(1) amendment defines **reporting requirements** as:

“(b) (1) A clinic, health facility, home health agency, or hospice ..... shall report any unlawful or **unauthorized** access to, or use or disclosure of, a patient's medical information to the department no later than **fifteen business days** after the unlawful or unauthorized access, use, or disclosure has been **detected** by the clinic, health facility, home health agency, or hospice.”

Cal. Health & Safety Code §1280.15(i)(2) defines **unauthorized** access as:

“the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (CMIA) . . . or any other statutes or regulations governing the lawful access, use, or disclosure of medical information.”
Recommendations for Handling Patient Information
**When Sending Faxes:**

- Pre-program or periodically check fax numbers
- Call intended recipient before sending the fax
- Double-check the fax number before sending
- Use MHS approved fax coversheet (can be found on the MHS Compliance and Business Ethics Website)
- Report misdirected faxes to the Compliance Department (i.e. you are contacted and told. "you sent the fax to the wrong number," ask the person calling "to fax the documents back to you and provide the information to the Compliance Department with this notification (phone 714-377-3218; fax 714-377-3225) and/or enter a “HIPAA” MemSafe event through the Risk Management reporting system (MemSafe)
Faxing Guidelines
Continued

**Receiving Faxes:**
- Place fax machine in a secure area to avoid unauthorized individuals from viewing
- Tell the person faxing information to warn you ahead of time
- Take faxes off the machine immediately
- Do not leave faxed patient information laying around unattended

**Verification Prior to Faxing:**
- Request patient identifying information; standard practice is two elements (i.e. Name, DOB, Address) but can include more if needed to determine that the request is appropriate
- If necessary, have the individual making the request submit the request in writing (ex. company letterhead with patient information being requested)
- Scenarios involving court documents, legal custody, power of attorney, etc., involve Medical Records/HIM or Compliance as a resource to determine appropriateness of request for release
Document Disposal

Anything with patient information or marked as confidential must be disposed of in the “grey” secured/confidential bins that are emptied and destroyed daily.

If you are unsure about the sensitivity of the document, check with your immediate supervisor.
Patient care areas are fast paced environments that involve releasing care plans, discharge instructions, prescriptions etc. to patients throughout the continuum of care. For this reason, it is important to take a “Patient Information Time-out” to ensure that before releasing information to an individual that you have verified that it is the correct patient and the information being released is for that patient only.

**Patient verification**
Request patient identifying information; standard practice is two identifiers, but can include more if needed. When verifying name, please verify first and last name.

**Document verification**
When taking information from a printer or work area, stop and check each page before releasing the information. When “labeling” paperwork, double check to ensure that the medical information and the label/sticker are for the same patient.
Disclosing or sharing passwords is not allowed and against MHS policy #126 Responsible Use of Technology.

Contact the MHS Service Desk if you have any problems logging into a system.

Change your password if you suspect that your login has been compromised.

Follow the established password guidelines (P&P #126, section13.2):

a) The most secure passwords are those that contain a combination of alphabetic, numeric, and special characters. Consider using special characters to break up small common words: “my$house” or “the@red&car.”

b) The password should be changed whenever a compromise of the password is suspected or after any period defined by MHS policy.

c) Passwords should not be associated with personal information (e.g., PIN used for bank cards, date of birth for self or family members, telephone numbers, first or last name of self or family members, passwords used for Internet accounts).

**REMEMBER: MemorialCare will never ask for your password!!!**
MemorialCare and other healthcare providers are under “attack” daily by sophisticated cyber-attacks, email phishing-attacks and cyber criminals. Many of these attacks have been successful, resulting in reputational harm, financial harm, fines and audits.

What can you do to prevent cyber-attacks and email Phishing Scams?

• Never divulge your password to anyone. MemorialCare will never ask you for your password. The only one asking for your password are cyber-criminals.
• If you receive an email asking you for your username or password DELETE it.
• It is against MemorialCare policy for anyone to print, store on-line, or give their password to others.
• Never click on a suspicious link from an unknown sender, or open a document or attachment from an unknown sender or suspicious sender.
• Immediately report to the MHS Service Desk (562-933-9450) any suspicious activity on any of your accounts, or any suspicious email that you might receive.
Phishing attacks have become more sophisticated. Here is an example of a spear phishing email. Spear Phishing is a highly targeted phishing attempt.

The attacker selectively chooses the recipient (target) and usually has a thorough understanding of the target’s organization.

The attacker may:

- Address the recipient by name
- Use lingo/jargon of the organization
- Reference actual departments, individuals and logos

The email may appear very genuine. Sometime these emails have legitimate terms and key words in the subject and body of the message.
MHS policy prohibits accessing patient information unless it is for an authorized business need (treatment, payment or healthcare operations).

Our policy also prohibits accessing your own medical record (self access).

The discovery and confirmation of unauthorized access is a “reportable event” by California Law and the Office for Civil Rights and may be subject to fines and penalties.
Inappropriate Access of Patient Records

Accessing the medical records of your children, family members and/or friends is not allowed unless you have a business or operational reason to do so.

The MemorialCare Compliance department conducts proactive monthly auditing and monitoring of systems that contain PHI. Those who violate HIPAA can be subject to disciplinary action.
Use of Personal Email Accounts (Cox, Gmail, Yahoo, AOL, etc.)

Use of a personal, non-MHS provided or non-MHS email account through an MHS network resource or owned device is generally discouraged, and must be infrequent, irregular, and temporary.

• Sending email **from a personal email** account while at work or while connected MHS.
  • **Users are prohibited from using a personal email address or account to send any message containing PHI, PII, Confidential/Proprietary Information.**

• Sending email **to a personal email account** while at work or while connected to MHS.
  • **Users are prohibited from using their MHS email account to send any message containing PHI, PII, Confidential/Proprietary Information to their personal account**

• Sending PHI or PII from a MHS email to a recipient who uses a personal email account.
  • **Users may use their MHS email account to send PHI or PII for appropriate business purposes to a business recipient’s personal email account only if the following requirements are met:**
    - The subject line must NOT contain any identifiable PHI or PII
    - Include “ZDSECURE” anywhere in the subject line to encrypt the message
    - Avoid sending any mental health, substance abuse or HIV information.
    - Email that includes PHI or PII must only contain the minimum necessary PHI or PII. Users should remove PHI and PII that is not necessary.

For more information see P&P #126 Responsible Use of Technology – Section 10
When using or disclosing PHI, all MHS workforce members will make reasonable efforts to limit the PHI used or disclosed to the minimum necessary to accomplish the intended purpose of the use or disclosure.

Instances where minimum necessary standard does not apply:
- PHI is for use by or a disclosure to a healthcare provider for treatment purposes
- Disclosure is to the patient or the patient's legally authorized representative
- Disclosure is pursuant to a valid authorization, in which case, the disclosure will be limited to the PHI specified on the authorization
- Disclosure is to the Secretary of Health and Human Services
- Disclosure is required by law.
If you or your department needs to dispose of electronic PHI, contact the MHS Service Desk for specific instructions.

Patient information in an electronic format requires the same safeguards as printed information.

You also need to discuss this with your supervisor because there may be specific regulations that address record retention.
MemorialCare has an obligation under HIPAA & CA Law to implement physical and technical safeguards.

- Remember to log off or secure your computer when you are leaving your work station. “\texttt{ctrl+alt+del when you leave your seat}”!

- Be mindful of what private information others might see when using computers in public areas.
MHS policy prohibits at all times, the use of a mobile device to text, transmit, receive or store any Protected Health Information (PHI) in any form or medium or photograph any individual receiving care and treatment in a MemorialCare facility.

For more information please reference P&P #126 Responsible Use of Technology and P&P # 195 Photography, Videography and Audiography
Users granted access to portable Technology Resources (personal computers, laptops, electronic tablets, iPads, iPhones) are responsible for ensuring that unauthorized persons are prevented from using or accessing such devices for any purpose. Any unauthorized access to Protected Health Information (PHI) is a reportable breach.

In particular, portable Technology Resources, should never be left unattended in any uncontrolled environment, including but not limited to:

- Unattended in a car overnight
- A vendor’s facility or vendor location
- Any public area (Restaurant, Starbucks, Hotel Lobby, etc.)

If any portable Technology Resource is lost or stolen, or if a User believes that a password has been compromised, report the incident immediately to the MHS Service Desk at 562-933-9450
Where do I get additional information or who can I ask if my questions are not answered?

- Immediate Supervisor
- MHS Intranet
  - Policies/Procedures
  - MHS Links – Compliance Resource Center

Compliance Department: 714-377-3218
Ethics Hotline: 888-933-9044
E-mail: ethicshotline@memorialcare.org
IMPORTANT NOTICE

This training module will assist Medicare Parts C and D plan Sponsors in satisfying the Compliance training requirements of the Compliance Program regulations at 42 C.F.R. §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi) and in Section 50.3 of the Compliance Program Guidelines found in Chapter 9 of the Medicare Prescription Drug Benefit Manual and Chapter 21 of the Medicare Managed Care Manual.

While Sponsors may choose to use this module to satisfy compliance training requirements, completion of this training in and of itself does not ensure that a Sponsor has an “effective Compliance Program.” Sponsors are responsible for ensuring the establishment and implementation of an effective Compliance Program in accordance with CMS regulations and program guidelines.
Why Do I Need Training?

Compliance is EVERYONE’S responsibility! As an individual who provides health or administrative services for Medicare enrollees, every action you take potentially affects Medicare enrollees, the Medicare program, or the Medicare trust fund.

Training Objectives:

- To understand the organization’s commitment to ethical business behavior
- To understand how a compliance program operates
- To gain awareness of how compliance violations should be reported
Where Do I Fit in the Medicare Program?
Background

• CMS requires Medicare Advantage, Medicare Advantage-Prescription Drug, and Prescription Drug Plan Sponsors (“Sponsors”) to implement an effective compliance program.

• An effective compliance program should:
  • Provide guidance on how to identify and report compliance violations
  • Provide guidance on how to handle compliance questions and concerns
  • Articulate and demonstrate an organization’s commitment to legal and ethical conduct
Compliance

A culture of compliance within an organization:
- Prevents noncompliance - Detects noncompliance - Corrects noncompliance

At a minimum, a compliance program must include the 7 core requirements:

1) Written Policies, Procedures and Standards of Conduct;
2) Compliance Officer, Compliance Committee and High Level Oversight;
3) Effective Training and Education;
4) Effective Lines of Communication;
5) Well Publicized Disciplinary Standards;
6) Effective System for Routine Monitoring and Identification of Compliance Risks; and
7) Procedures and System for Prompt Response to Compliance Issues

42 C.F.R. §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi); Internet-Only Manual (“IOM”), Pub. 100-16, Medicare Managed Care Manual Chapter 21; IOM, Pub. 100-18, Medicare Prescription Drug Benefit Manual Chapter 9
CMS expects that all Sponsors will apply their training requirements and “effective lines of communication” to the entities with which they partner.

Having “effective lines of communication” means that employees of the organization and the partnering entities have several avenues through which to report compliance concerns.

Ethics – Do the Right Thing

- Act Fairly and Honestly
- Comply with the letter and spirit of the law
- Adhere to high ethical standards in all that you do
- Report suspected violations

As a part of the Medicare program, it is important that you conduct yourself in an ethical and legal manner. It’s about doing the right thing!
How Do I Know What is Expected of Me?

Standards of Conduct (or Code of Conduct) state compliance expectations and the principles and values by which an organization operates.

Contents will vary as Standards of Conduct should be tailored to each individual organization’s culture and business operations.

*Everyone* is required to report violations of Standards of Conduct and suspected noncompliance.

An organization’s Standards of Conduct and Policies and Procedures should identify this obligation and tell you how to report.
CMS Mandated Compliance Training; Medicare Parts C&D

What is Noncompliance?

Noncompliance is conduct that does not conform to the law, and Federal health care program requirements, or to an organization's ethical and business policies.

* For more information, see the Medicare Managed Care Manual and the Medicare Prescription Drug Benefit Manual on [http://www.cms.gov](http://www.cms.gov)
Noncompliance Harms Enrollees

Without programs to prevent, detect, and correct noncompliance there are:

- Delayed services
- Denial of Benefits
- Hurdles to care
- Difficulty in using providers of choice

Noncompliance Costs Money

Non Compliance affects EVERYBODY!
Without programs to prevent, detect, and correct noncompliance you risk:

- Higher Premiums
- Higher Insurance Copayments
- Lower profits
- Lower benefits for individuals and employers
- Lower Star ratings
CMS Mandated Compliance Training; Medicare Parts C&D

I’m Afraid to Report Noncompliance:

There can be **NO** retaliation against you for reporting suspected noncompliance in good faith. Each Sponsor must offer reporting methods that are:

- Confidential
- Anonymous
- Non-Retalatory

How Can I Report Potential Noncompliance?

- **Employees of an MA, MA-PD, or PDP Sponsor**
  - Call the Medicare Compliance Officer
  - Make a report through the Website
  - Call the Compliance Hotline

- **FDR Employees**
  - Talk to a Manager or Supervisor
  - Call Your Ethics/Compliance Help Line
  - Report through the Sponsor

- **Beneficiaries**
  - Call the Sponsor’s compliance hotline
  - Make a report through Sponsor’s website
  - Call 1-800-Medicare
CMS Mandated Compliance Training; Medicare Parts C&D

What Happens Next?

- After noncompliance has been detected...
- It must be investigated *immediately*...
- And then *promptly* correct any noncompliance

Correcting Noncompliance

- Avoids the recurrence of the same noncompliance
- Promotes efficiency and effective internal controls
  - Protects enrollees
    - Ensures ongoing compliance with CMS requirements
How Do I Know the Noncompliance Won't Happen Again?

- Once noncompliance is detected and corrected, an ongoing evaluation process is critical to ensure the noncompliance does not recur.
- Monitoring activities are regular reviews which confirm ongoing compliance and ensure that corrective actions are undertaken and effective.
- Auditing is a formal review of compliance with a particular set of standards (e.g., policies and procedures, laws and regulations) used as base measures.
CMS Mandated Compliance Training; Medicare Parts C&D

Know the Consequences of Noncompliance:

Your organization is required to have disciplinary standards in place for non-compliant behavior. Those who engage in non-Compliant behavior may be subject to any of the following:

- Mandatory Training or Re-Training
- Disciplinary Action
- Termination

Compliance is EVERYONE’S Responsibility!!

PREVENT
- Operate within your organization’s ethical expectations to PREVENT noncompliance!

DETECT & REPORT
- If you DETECT potential noncompliance, REPORT it!

CORRECT
- CORRECT noncompliance to protect beneficiaries and to save money!
Case Scenario 1:
You have discovered an unattended email address or fax machine in your office which receives beneficiary appeals requests. You suspect that no one is processing the appeals. What should you do?

A) Contact Law Enforcement
B) Nothing
C) Contact your Compliance Department
D) Wait to confirm someone is processing the appeals before taking further action
E) Contact your supervisor

The correct answer is: C – Contact your Compliance Department.
Suspected or actual noncompliance should be reported immediately upon discovery. It is best to report anything that is suspected rather than wait and let the situation play out.

Your Sponsor’s compliance department will have properly trained individuals who can investigate the situation and then, as needed, take steps to correct the situation according to the Sponsor’s Standards of Conduct and Policies and Procedures.
Case Scenario 2:
A sales agent, employed by the Sponsor's first-tier or downstream entity, has submitted an application for processing and has requested two things:
   i) the enrollment date be back-dated by one month
   ii) all monthly premiums for the beneficiary be waived

What should you do?

A. Refuse to change the date or waive the premiums, but decide not to mention the request to a supervisor or the compliance department
B. Make the requested changes because the sales agent is responsible for determining the beneficiary's start date and monthly premiums
C. Tell the sales agent you will take care of it, but then process the application properly (without the requested revisions). You will not file a report because you don't want the sales agent to retaliate against you
D. Process the application properly (without the requested revisions). Inform your supervisor and the compliance officer about the sales agent's request.
E. Contact law enforcement and CMS to report the sales agent's behavior.
Case Scenario 2:
The correct answer is: D - Process the application properly (without the requested revisions). Inform your supervisor and the compliance officer about the sales agent's request.

The enrollment application should be processed in compliance with CMS regulations and guidance. If you are unclear about the appropriate procedure, then you can ask your supervisor or the compliance department for additional, job-specific training.

Your supervisor and the compliance department should be made aware of the sales agent's request so that proper retraining and any necessary disciplinary action can be taken to ensure that this behavior does not continue. No one, including the sales agent, your supervisor, or the Compliance Department, can retaliate against you for a report of noncompliance made in good faith.
Case Scenario 3:
You work for an MA-PD Sponsor. Last month, while reviewing a monthly report from CMS, you identified multiple enrollees for which the Sponsor is being paid, who are not enrolled in the plan.

You spoke to your supervisor, Tom, who said not to worry about it. This month, you have identified the same enrollees on the report again.

What do you do?
A) Decide not to worry about it as your supervisor, Tom, had instructed. You notified him last month and now it’s his responsibility.
B) Although you have seen notices about the Sponsor’s non-retaliation policy, you are still nervous about reporting. To be safe, you submit a report through your Compliance Department’s anonymous tip line so that you cannot be identified.
C) Wait until next month to see if the same enrollees are on the report again, figuring it may take a few months for CMS to reconcile its records. If they are, then you will say something to Tom again.
D) Contact law enforcement and CMS to report the discrepancy.
E) Ask Tom about the discrepancies again.
Case Scenario 3:

The correct answer is: B - Although you have seen notices about the Sponsor’s non-retaliation policy, you are still nervous about reporting. To be safe, you submit a report through your Compliance Department’s anonymous tip line so that you cannot be identified.

There can be no retaliation for reports of noncompliance made in good faith. To help promote reporting, Sponsors should have easy-to-use, confidential reporting mechanisms available to its employees 24 hours a day, 7 days a week. MemorialCare’s Ethics Hotline is (888) 933-9044 or you can send an email to EthicsHotline@memorialcare.org

It is best to report any suspected noncompliance to the Compliance Department promptly to ensure that the Sponsor remains in compliance with CMS requirements. Do the right thing! Compliance is everyone’s responsibility.
What Governs Compliance?

Social Security Act:
  • Title 18

Code of Federal Regulations*:
  • 42 CFR Parts 422 (Part C) and 423 (Part D)

CMS Guidance:
  • Manuals
  • HPMS Memos

CMS Contracts:
  • Private entities apply and contracts are renewed/non-renewed each year

Other Sources:
  • OIG/DOJ (fraud, waste and abuse (FWA))
  • HHS (HIPAA privacy)

State Laws:
  • Licensure
  • Financial Solvency
  • Sales Agents

* 42 C.F.R. §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)
Additional Resources

For more information on laws governing the Medicare program and Medicare noncompliance, or for additional healthcare compliance resources please see:

- Title XVIII of the Social Security Act
- Medicare Regulations governing Parts C and D (42 C.F.R. §§ 422 and 423)
- Civil False Claims Act (31 U.S.C. §§ 3729-3733)
- Criminal False Claims Statute (18 U.S.C. §§ 287,1001)
- Anti-Kickback Statute (42 U.S.C. § 1320a-7b(b))
- Exclusion entities instruction (42 U.S.C. § 1395w-27(g)(1)(G))
As part of MemorialCare’s workforce, I have been trained on and understand the compliance requirements and responsibilities as they relate to my job function. My job responsibilities include ensuring that MemorialCare remains compliant with all applicable Federal and State health care program requirements, Policies and Procedures, and I have taken steps to promote such compliance. To the best of my knowledge my job function and duties are in compliance with all applicable Federal and State health care program requirements. I understand that this certification is being provided to and relied upon by MemorialCare and those we do business with.
Congratulations!

You have completed the Centers for Medicare & Medicaid Services Parts C & D Compliance Training

And

MemorialCare’s FY’16 Annual Compliance Training

You will now need to complete the quiz portion of this course to receive credit of completion.