MemorialCare™

Annual Corporate Compliance Training

2021

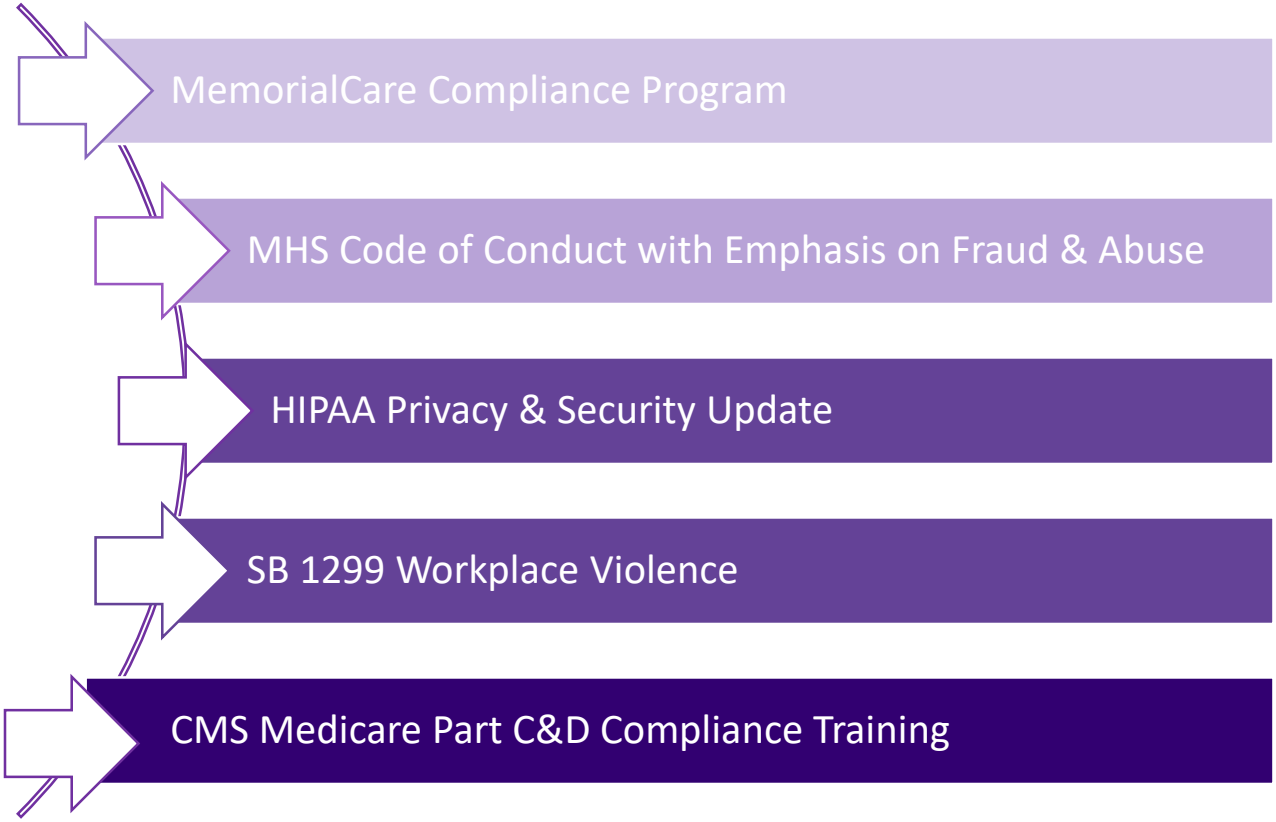
Introduction

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.

MemorialCare™

Compliance Training Overview



MemorialCare™

“Compliance is Everyone’s Business”

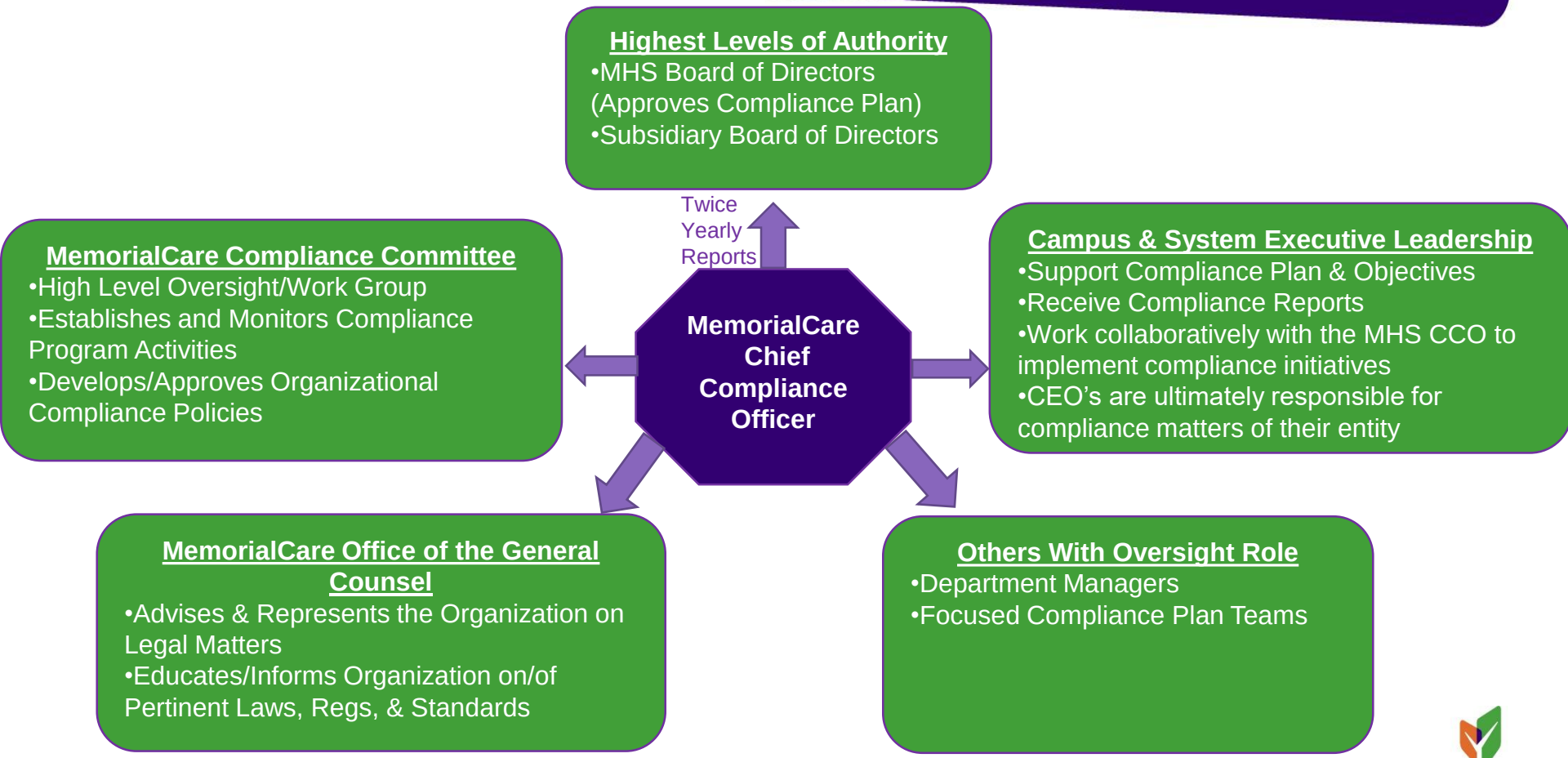
MemorialCare has a compliance program in place to bring awareness to its workforce in regard to following regulations, policies, procedures and the MHS Code of Conduct. This makes compliance the responsibility of everyone.

MemorialCare™

Key Elements of MemorialCare's Compliance Program

MemorialCare™

MemorialCare Compliance Oversight Structure



MemorialCare™

Compliance Team

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

Ann Mason
Director of Compliance
Amason@memorialcare.org
714-377-3226

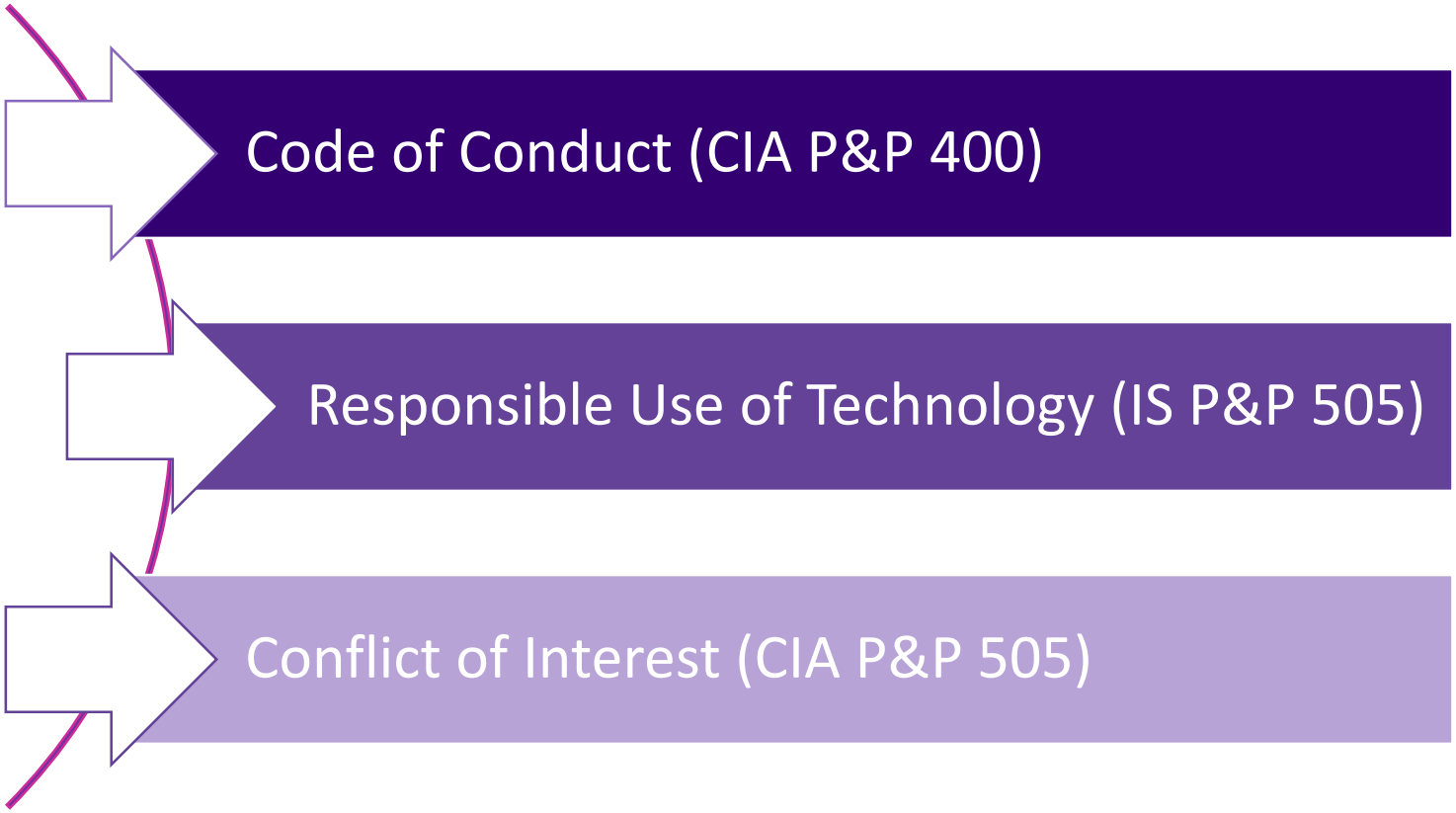
Tina Cordell
Compliance Manager
Tcordell@memorialcare.org
714-377-3237

Carla Garcia
Compliance & Appeals Coordinator
Cgarcia7@memorialcare.org
714-377-3216

Catherine Vu
Compliance Coordinator
Cvu5@memorialcare.org
714-377-3205

MemorialCare™

Key Compliance Policies & Procedures



MemorialCare™

Code of Conduct

MemorialCare™

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.

MemorialCare™

Code of Conduct

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

MemorialCare™

Code of Conduct

Legal Compliance

MemorialCare intends that all activities will be in compliance with applicable laws and regulatory standards. Next 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 staff 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.

MemorialCare™

Code of Conduct

Legal Compliance: Fraud & 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.

MemorialCare™

Code of Conduct

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.

MemorialCare™

Code of Conduct

Legal Compliance: False Claims Act Cont.

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
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.

MemorialCare™

Code of Conduct

CMS 60-Day Overpayment Rule

Legal Compliance: CMS 60-Day Overpayment Rule

In the event of an overpayment from Medicare or Medicaid, MemorialCare shall report and return the overpayment within the latter of (1) 60 days after the date on which the payment was identified and (2) the due date of any corresponding cost report. If you are aware of an overpayment or potential overpayment, notify your supervisor.

MemorialCare

Code of Conduct

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, or the CMS 60-day Overpayment rule. We encourage you to report any suspected violations of these, or any other laws described in the Code of Conduct.

MemorialCare™

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.

MemorialCare™

Code of Conduct

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, timecards, medical records, and benefit forms.

MemorialCare™

Code of Conduct

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.

MemorialCare™

Code of Conduct

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.

MemorialCare™

Code of Conduct

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's 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

MemorialCare™

Code of Conduct

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.

MemorialCare™

Code of Conduct

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.

MemorialCare™

Code of Conduct

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.

MemorialCare™

Code of Conduct

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 CIA 408

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.

MemorialCare™

Code of Conduct
Compliance & Ethics Hotline

If you have any question or are aware of behavior that is not consistent with MemorialCare's mission, values, Code of Conduct, policies, or laws and regulations, you are encouraged to report your concerns to your manager or to MemorialCare's Chief Compliance and Audit Officer at 714-377-3218.

You can also report your concern anonymously by calling or emailing the Compliance & Ethics Hotline. MemorialCare policy prohibits retaliation against individuals who report issues and concerns in good faith.

Compliance & Ethics Hotline

Available 24/7, 365 days of the year

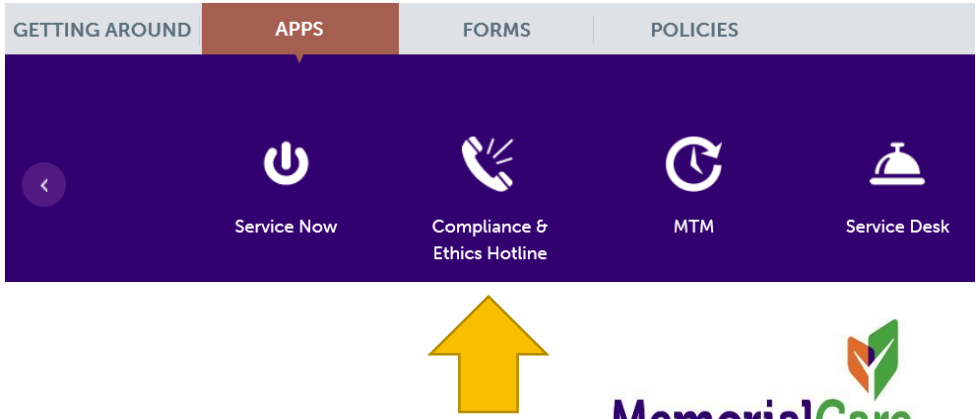
Dial toll-free: 888-933-9044

OR

Online: memorialcare.ethicspoint.com

OR

On the IntraNet:



MemorialCare

HIPAA Privacy & Security Update

MemorialCare™

HIPAA and Patient Privacy

The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996 (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™

California Privacy Rules

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!

California Health & Safety Codes

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."

MemorialCare™

Examples of a Potential Breach

The following are examples of a potential breach that should be reported in MemSafe:

- Misdirected fax or email
- Patient given documentation for the wrong patient
- Patient scheduled or checked in under a different patient account
- Snooping in a patient chart
- Mislabeled specimens or documents
- Lost/stolen company device, such as laptop or iPhone
- Improper disposal of PHI (PHI found in regular trash, bathroom, parking lot, etc.)
- Password violation, such as password sharing

MemorialCare™

Information Blocking

What is it?

The 21st Century Cures Act became law on December 13th, 2016. This law establishes programs and oversight to promote the exchange of health information and to prohibit "information blocking" practices.

In general, information blocking is a practice by a health IT developer of certified health IT, health information network, health information exchange, or health care provider that, except as required by law or specified by the Secretary of Health and Human Services (HHS) as a reasonable and necessary activity, is likely to interfere with access, exchange, or use of electronic health information (EHI).

Have questions about information blocking? View our Information Blocking Frequently Asked Questions (FAQs)

MemorialCare policy

MemorialCare Health System will not knowingly interfere with access, exchange, or use of EHI unless the practice is required by law or a Regulatory Exception applies.

MemorialCare™

Information Blocking

What are examples of practices that could constitute information blocking?

•Practices that restrict authorized access, exchange, or use under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law, including transitions between certified health information technologies (health IT);

•Implementing health IT in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using EHI;

•Implementing health IT in ways that are likely to—

- Restrict the access, exchange, or use of EHI with respect to exporting complete information sets or in transitioning between health IT systems; or
- Lead to fraud, waste, or abuse, or impede innovations and advancements in health information access, exchange, and use, including care delivery enabled by health IT.

For additional examples of practices that *could* constitute information blocking go to ONC's Cures Act Final Rule.

MemorialCare™

Information Blocking

Reporting Potential Information Blocking Practices

- Any employee, physician, contractor or volunteer who learns of a practice that interferes with a third party's access, exchange, or use of EHI should immediately report the practice to The Chief Compliance Officer by calling the Compliance and Ethics Hotline at 888-933-9044.

MemorialCare™

Recommendations for Handling Patient Information

MemorialCare™

Faxing Guidelines

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)

MemorialCare™

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

MemorialCare™

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.

If working from home and printing PHI, you must use a shredder to destroy any printed documents. Ask your supervisor how to order one if needed.

MemorialCare™

Patient Information in the Work Area

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. A minimum of two identifiers should always be used. 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.

MemorialCare™

Sharing Passwords

Disclosing or sharing passwords is not allowed and against MHS IS policy #505 Responsible Use of Technology.

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

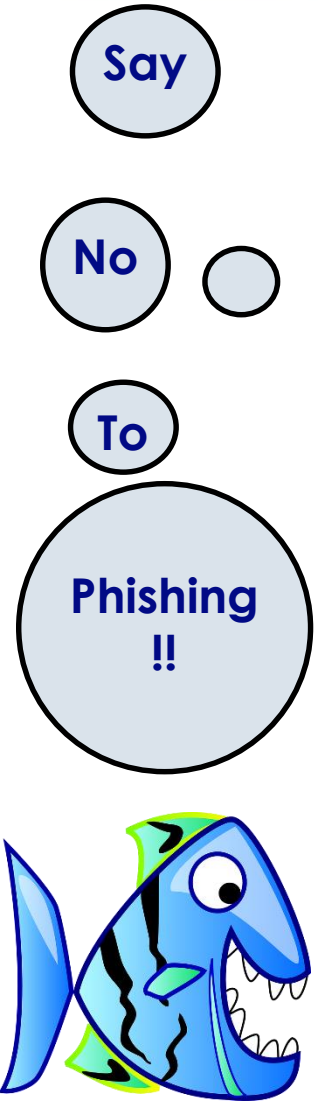
Change your password if you suspect that your login has been compromised.

Follow the established password guidelines (IS #505, 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).

MemorialCare™

Phishing Attacks



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.

MemorialCare™

Inappropriate Access of Patient Records

- 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.

MemorialCare™

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.

MemorialCare™

Use of Personal Email Accounts

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.

MemorialCare

PHI: Minimum Necessary Standard P&P
CIA 469

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.

MemorialCare™

Disposing of Electronic Media with PHI

- 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™

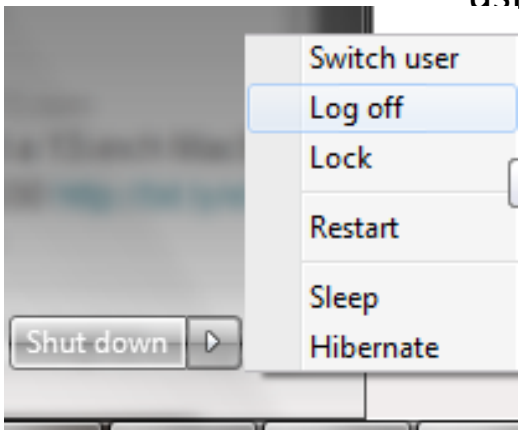
Computer Terminal Security / Auto Log-offs

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 workstation.

“ctrl+alt+del when you leave your seat”!

- Be mindful of what private information others might see when using computers in public areas.



MemorialCare™

Portable Computing Devices Security

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**

MemorialCare™

Need Help?

Where do I get additional information or who can I ask if my questions are not answered?

- Immediate Supervisor
- MemorialCare Intranet
  - ✓ Policies/Procedures
  - ✓ MCSS Compliance department page
- Compliance Department: 714-377-3218
- Ethics Hotline: 888-933 -9044
- E-mail: ethicshotline@memorialcare.org

MemorialCare™

SB-1299 Workplace Violence

Workplace Violence Prevention Plan

MemorialCare™

Overview

- Introduction to the Workplace Violence Prevention Plan
- Recognizing the potential for violence
- How to respond to risks of violence / reporting
- How to avoid harm
- Notification plans – understanding alerts and alarms.
- Public Safety / Security Teams
- Post-incident resources
- How to obtain additional information

MemorialCare™

Workplace Violence Prevention

Workplace Violence Prevention Plan

- All members of the MemorialCare workforce are entitled to a workplace free of acts of violence. This includes physical acts of violence, and acts of force thru intimidation, harassment and verbal abuse.
- Worksites are regularly evaluated for safety and security risks; identified risks are reduced as much as possible.
- Risk evaluation strategies include routine hazard observation rounds, patient risk evaluations, violence incident reports and investigations, and more.
- Different lessening strategies are in place, including security personnel and systems, routine training on workplace violence prevention, workflow and space design.

MemorialCare™

Workplace Violence Prevention

Workplace Violence Prevention Plan

- All patients are to be evaluated for their risk of violence upon arrival in our healthcare setting.
- Prevention and lessening strategies may vary by location.
- Report all identified risks or acts of violence to Public Safety and/or management as soon as possible. (Also report in MemSafe)
- All reports of risk or acts of violence will be acted upon without retaliation to the individual making the report.
- Communicate all security/safety concerns to management and/or Public Safety immediately.
- MemorialCare makes every effort to identify and reduce all safety risks.
- MemorialCare maintains zero tolerance for violent behavior.

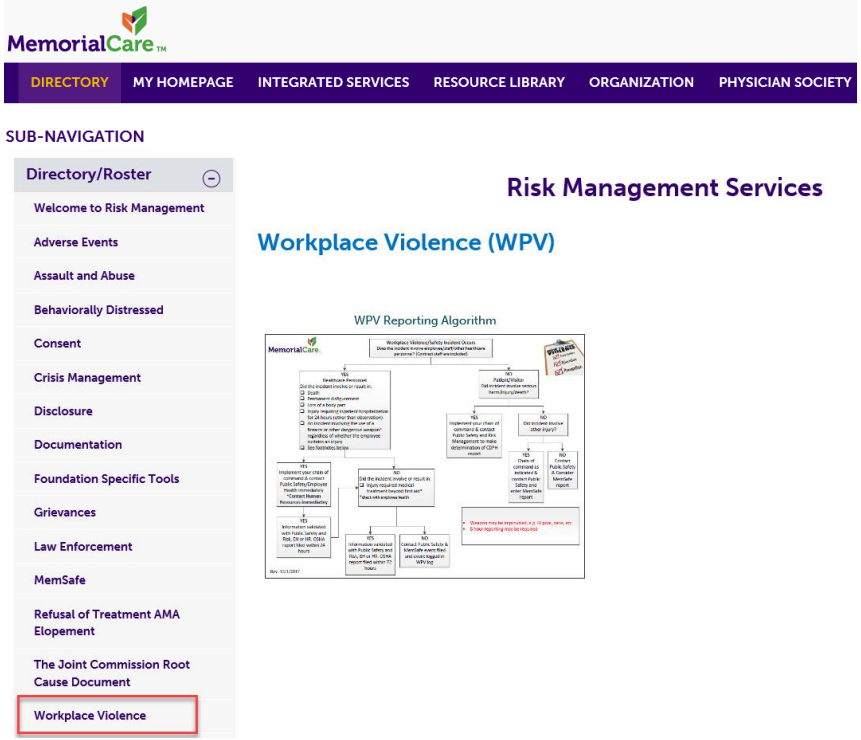
MemorialCare™

Workplace Violence Prevention

Workplace Violence Prevention Plan

- **Find additional details, you may review and provide feedback on MemorialCare's Workplace Violence Prevention Plan located on the intranet:**

https://memorialcare.sharepoint.com/sites/07a/MCSS_risk_management/Pages/Home.aspx



MemorialCare

Workplace Violence Prevention

Recognizing the potential for violence

- Risk factors: history of violent behavior, drug/alcohol use, behavioral health disorders, dementia, extreme anxiety/stress, etc.
- Warning signs: elevated voice, anger; perception of unfair treatment or hostility; paranoia; pacing; clenched fists; sweating.
- Employee: use calm voice; seek cooperation and agreement. Request assistance if needed.
- Measures to maximize your personal safety include: knowledge of your surroundings, identifying and maintaining a path of escape, removing hazardous items and make do weapons from at-risk patients, safety in numbers, use of de-increase ways of doing things.
- Report to Public Safety or management immediately.

MemorialCare™

Workplace Violence Prevention

Facility Protocols:

Hospitals:

- Emergency codes (code gray, silver, pink, active shooter, etc.)
- Threat alarms in some locations.
- Public Safety teams responsible for maximizing safety and responding to security incidents.
- Call internal emergency hotline and/or 911.
- Escape routes / Shelter

Non-hospitals:

- Emergency codes
- Law enforcement responds to security incidents and acts of workplace violence. Call 911.

MemorialCare™

Workplace Violence Prevention

Follow up:

Post Incident:

- MemorialCare provides coping resources to all employees involved in workplace violence incidents.
- **REACH / Counseling available**
- All incidents will be investigated, including an opportunity for those affected to speak with investigators.

More questions / concerns?

- **Contact Public Safety or Human Resources for additional concerns or assistance.**

MemorialCare™

Medicare Parts C and D Fraud, Waste, and Abuse Training

MemorialCare™

INTRODUCTION

The Combating Medicare Parts C and D Fraud, Waste, and Abuse Web-Based Training course is brought to you by the Medicare Learning Network®, a registered trademark of the U.S. Department of Health & Human Services (HHS)

MemorialCare™

INTRODUCTION

This Web-Based Training (WBT) course was current at the time it was published or uploaded onto the web. Medicare policy changes frequently so links to the source documents have been provided within the WBT for your reference.

This WBT course was prepared as a service to the public and is not intended to grant rights or impose obligations. This WBT may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents. This training module will assist Medicare Parts C and D plan Sponsors employees, governing body members, and their first-tier, downstream, and related entities (FDRs) in satisfying the annual Fraud, Waste, and Abuse (FWA) training requirements in the regulations and sub-regulatory guidance at:

- 42 Code of Federal Regulations (CFR) Section 422.503(b)(4)(vi)(C);
- 42 CFR Section 423.504(b)(4)(vi)(C);
- CMS-4159-F, Medicare Program Contract Year 2015 Policy and Technical Changes in the Medicare Advantage and the Medicare Prescription Drug Benefit Programs; and
- Section 50.3.2 of the Compliance Program Guidelines (Chapter 9 of the “Medicare Prescription Drug Benefit Manual” and Chapter 21 of the “Medicare Managed Care Manual”).

Sponsors and their FDRs may use this module to satisfy FWA training requirements. Sponsors and their FDRs are responsible for providing additional specialized or refresher training on issues posing FWA risks based on the employee’s job function or business setting.

ACRONYM	Meaning
CFR	Code of Federal Regulations
FDR	First-Tier, Downstream, or Related Entity
FWA	Fraud, Waste, and Abuse
WBT	Web-based training

MemorialCare™

INTRODUCTION

Welcome to the **Medicare Learning Network® (MLN)** – Your free Medicare education and information resource!
The MLN is home for education, information, and resources for the health care professional community. The MLN provides access to the Centers for Medicare & Medicaid Services (CMS) Program information you need, when you need it, so you can focus more on providing care to your patients.
Serving as the umbrella for a variety of CMS education and communication activities, the MLN offers:

1. MLN Educational Products, including MLN Matters® Articles;
2. Web-Based Training (WBT) Courses (many offer Continuing Education credits);
3. MLN Connects® National Provider Calls;
4. MLN Connects® Provider Association Partnerships;
5. MLN Connects® Provider eNews;
6. Provider electronic mailing lists.

ACRONYM	Meaning
CMS	Centers for Medicaid and Medicare Services
MLN	Medicare Learning Network®

Why Do I Need Training?
Every year **billions** of dollars are improperly spent because of FWA. It affects everyone – **including you.** This training will help you detect, correct, and prevent FWA. **You** are part of the solution.

Combating FWA 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.

MemorialCare™

INTRODUCTION

Training Requirements: Plan Employees, Governing Body Members, and First-Tier, Downstream, or Related Entity (FDR) Employees

Certain training requirements apply to people involved in Medicare Parts C and D. All employees of Medicare Advantage Organizations (MAOs) and Prescription Drug Plans (PDPs) (collectively referred to in this WBT course as "Sponsors") must receive training for preventing, detecting, and correcting FWA.

FWA training must occur within 90 days of initial hire and at least annually thereafter.
More information on other Medicare Parts C and D compliance trainings and answers to common questions is available on the CMS website.

FWA Training Requirements Exception

There is one exception to the FWA training and education requirement. FDRs will have met the FWA training and education requirements if they have met the FWA certification requirement through:

- Accreditation as a supplier of Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS); or
- Enrollment in Medicare Part A (hospital) or B (medical) Program.

If you are unsure if this exception applies to you, please contact your management team for more information.

ACRONYM	Meaning
MA	Medicare Advantage

MemorialCare™

INTRODUCTION

Course Objectives

When you complete this course, you should be able to correctly:

- Recognize FWA in the Medicare Program;
- Identify the major laws and regulations pertaining to FWA;
- Recognize potential consequences and penalties associated with violations;
- Identify methods of preventing FWA;
- Identify how to report FWA; and
- Recognize how to correct FWA.

MemorialCare™

LESSON 1: WHAT IS FWA?

Introduction and Learning Objectives

This lesson describes Fraud, Waste, and Abuse (FWA) and the laws that prohibit it. It should take about 10 minutes to complete. Upon completing the lesson, you should be able to correctly:

- Recognize FWA in the Medicare Program;
- Identify the major laws and regulations pertaining to FWA; and
- Recognize potential consequences and penalties associated with violations.

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.
The Health Care Fraud Statute makes it a criminal offense to knowingly and willfully execute a scheme to defraud a health care benefit program. Health care fraud is punishable by imprisonment for up to 10 years.
It is also subject to criminal fines of up to $250,000.

ACRONYM	Meaning
FWA	Fraud, Waste, and Abuse

MemorialCare™

LESSON 1: WHAT IS FWA?

Waste and Abuse

Waste includes overusing services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare Program. 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 not legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

*For the definitions of fraud, waste, and abuse, refer to Chapter 21, Section 20 of the "Medicare Managed Care Manual" and Chapter 9 of the "Prescription Drug Benefit Manual" on the Centers for Medicare & Medicaid Services (CMS) website.

Examples of FWA

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

- Knowingly billing for services not furnished or supplies not provided, including billing Medicare for appointments that the patient failed to keep;
- Billing for non-existent prescriptions; and
- Knowingly altering claim forms, medical records, or receipts to receive a higher payment.

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

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

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

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

MemorialCare™

LESSON 1: WHAT IS FWA?

Differences Among Fraud, Waste, and Abuse

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.

Understanding FWA

To detect FWA, you need to know the **law**.

The following screens provide high-level information about the following laws:

- Civil False Claims Act, Health Care Fraud Statute, and Criminal Fraud;
- Anti-Kickback Statute;
- Stark Statute (Physician Self-Referral Law);
- Exclusion; and
- Health Insurance Portability and Accountability Act (HIPAA).

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

MemorialCare™

LESSON 1-Civil False Claims Act (FCA)

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

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

For more information, refer to 31 United States Code (U.S.C.) Sections 3729-3733 on the Internet.

EXAMPLE

A Medicare Part C plan in Florida:

- Hired an outside company to review medical records to find additional diagnosis codes that could be submitted to increase risk capitation payments from the Centers for Medicare & Medicaid Services (CMS);
- Was informed by the outside company that certain diagnosis codes previously submitted to Medicare were undocumented or unsupported;
- Failed to report the unsupported diagnosis codes to Medicare; and
- Agreed to pay $22.6 million to settle FCA allegations.

Damages and Penalties

Any person who knowingly submits false claims to the Government is liable for three times the Government's damages caused by the violator plus a penalty.

ACRONYM	Meaning
FCA	False Claims Act

MemorialCare™

Whistleblowers

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

Protected: Persons who report false claims or bring legal actions to recover money paid on false claims are protected from retaliation.

Rewarded: Persons who bring a successful whistleblower lawsuit receive at least 15 percent but not more than 30 percent of the money collected.

Health Care Fraud Statute

The Health Care Fraud Statute states that "Whoever knowingly and willfully executes, or attempts to execute, a scheme to … defraud any health care benefit program … shall be fined … or imprisoned not more than 10 years, or both." Conviction under the statute does not require proof that the violator had knowledge of the law or specific intent to violate the law. For more information, refer to 18 U.S.C. Section 1346 on the Internet.

EXAMPLE

A Pennsylvania pharmacist:

- Submitted claims to a Medicare Part D plan for non-existent prescriptions and for drugs not dispensed;
- Pleaded guilty to health care fraud; and
- Received a 15-month prison sentence and was ordered to pay more than $166,000 in restitution to the plan.

The owners of two Florida Durable Medical Equipment (DME) companies:

- Submitted false claims of approximately $4 million to Medicare for products that were not authorized and not provided;
- Were convicted of making false claims, conspiracy, health care fraud, and wire fraud;
- Were sentenced to 54 months in prison; and
- Were ordered to pay more than $1.9 million in restitution.

MemorialCare™

LESSON 1 - Criminal Health Care Fraud

Criminal Health Care Fraud

Persons who knowingly make a false claim may be subject to:

- Criminal fines up to $250,000;
- Imprisonment for up to 20 years; or
- Both.

If the violations resulted in death, the individual may be imprisoned for any term of years or for life.
For more information, refer to 18 U.S.C. Section 1347 on the Internet.

Anti-Kickback Statute

The Anti-Kickback Statute prohibits knowingly and willfully soliciting, receiving, offering, or paying remuneration (including any kickback, bribe, or rebate) for referrals for services that are paid, in whole or in part, under a Federal health care program (including the Medicare Program).
For more information, refer to 42 U.S.C. Section 1320a-7b(b) on the Internet.

Damages and Penalties

Violations are punishable by:

- A fine of up to $25,000;
- Imprisonment for up to 5 years; or
- Both.

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

EXAMPLE

A radiologist who owned and served as medical director of a diagnostic testing center in New Jersey:

- Obtained nearly $2 million in payments from Medicare and Medicaid for MRIs, CAT scans, ultrasounds, and other resulting tests;
- Paid doctors for referring patients;
- Pleaded guilty to violating the Anti-Kickback Statute; and
- Was sentenced to 46 months in prison.

The radiologist was among 17 people, including 15 physicians, who have been convicted in connection with this scheme.

MemorialCare™

LESSON 1 -Stark Statute (Physician Self-Referral Law)

The Stark Statute prohibits a physician from making referrals for certain designated health services to an entity when the physician (or a member of his or her family) has:

- An ownership/investment interest; or
- A compensation arrangement (exceptions apply).

For more information, refer to 42 U.S.C. Section 1395nn on the Internet.

Damages and Penalties

Medicare claims tainted by an arrangement that does not comply with the Stark Statute are not payable. A penalty of around **$23,800** may be imposed for each service provided. There may also be around a **$159,000** fine for entering into an unlawful arrangement or scheme.

For more information, visit the Physician Self-Referral webpage on the CMS website and refer to the Act, Section 1877 on the Internet.

EXAMPLE

A physician paid the Government $203,000 to settle allegations that he violated the physician self-referral prohibition in the Stark Statute for routinely referring Medicare patients to an oxygen supply company he owned.

MemorialCare™

LESSON 1-Civil Monetary Penalties (CMP) Law

The Office of Inspector General (OIG) may impose civil penalties for a number of reasons, including:
- Arranging for services or items from an excluded individual or entity;
- Providing services or items while excluded;
- Failing to grant OIG timely access to records;
- Knowing of an overpayment and failing to report and return it;
- Making false claims; or
- Paying to influence referrals.

For more information, refer to 42 U.S.C. 1320a-7a and the Act, Section 1128A(a) on the Internet.

Damages and Penalties

The penalties can be around $15,000 to $70,000 depending on the specific violation. Violators are also subject to three times the amount:
- Claimed for each service or item; or
- Of remuneration offered, paid, solicited, or received.

EXAMPLE

A California pharmacy and its owner agreed to pay over $1.3 million to settle allegations they submitted claims to Medicare Part D for brand name prescription drugs that the pharmacy could not have dispensed based on inventory records.

ACRONYM	Meaning
OIG	Office of Inspector General

MemorialCare™

LESSON - Exclusion

No Federal health care program payment may be made for any item or service furnished, ordered, or prescribed by an individual or entity excluded by the OIG. The OIG has authority to exclude individuals and entities from federally funded health care programs and maintains the List of Excluded Individuals and Entities (LEIE). You can access the LEIE on the Internet.

The United States General Services Administration (GSA) administers the Excluded Parties List System (EPLS), which contains debarment actions taken by various Federal agencies, including the OIG. You may access the EPLS on the System for Award Management website.

If looking for excluded individuals or entities, make sure to check both the LEIE and the EPLS since the lists are not the same. For more information, refer to 42 U.S.C. Section 1320a-7 and 42 Code of Federal Regulations Section 1001.1901 on the Internet.

EXAMPLE

A pharmaceutical company pleaded guilty to two felony counts of criminal fraud related to failure to file required reports with the Food and Drug Administration concerning oversized morphine sulfate tablets. The executive of the pharmaceutical firm was excluded based on the company's guilty plea. At the time the executive was excluded, he had not been convicted himself, but there was evidence he was involved in misconduct leading to the company's conviction.

ACRONYM	Meaning
EPLS	Excluded Parties List System
LEIE	List of Excluded Individuals and Entities

MemorialCare™

LESSON 1
Health Insurance Portability and Accountability Act (HIPAA)

HIPAA created greater access to health care insurance, protection of privacy of health care data, and promoted standardization and efficiency in the health care industry.

HIPAA safeguards help prevent unauthorized access to protected health care information. As an individual with access to protected health care information, you must comply with HIPAA.

For more information, visit the HIPAA webpage on the Internet.

Damages and Penalties

Violations may result in Civil Monetary Penalties. In some cases, criminal penalties may apply.

EXAMPLE

A former hospital employee pleaded guilty to criminal HIPAA charges after obtaining protected health information with the intent to use it for personal gain. He was sentenced to 12 months and 1 day in prison.

ACRONYM	Meaning
HIPAA	Health Insurance Portability and Accountability Act

MemorialCare™

LESSON 1 SUMMARY

There are differences among FWA. One of the primary differences is intent and knowledge. Fraud requires that the person have intent to obtain payment and the knowledge that their actions are wrong. Waste and abuse may involve obtaining an improper payment but do not require the same intent and knowledge.
Laws and regulations exist that prohibit FWA. Penalties for violating these laws may include:

- Civil Monetary Penalties;
- Civil prosecution;
- Criminal conviction/fines;
- Exclusion from participation in all Federal health care programs;
- Imprisonment; or
- Loss of provider license.

MemorialCare™

LESSON 2: YOUR ROLE IN THE FIGHT AGAINST FWA

Introduction and Learning Objectives

This lesson explains the role you can play in fighting against Fraud, Waste, and Abuse (FWA), including your responsibilities for preventing, reporting, and correcting FWA. It should take about 10 minutes to complete.
Upon completing the lesson, you should be able to correctly:

- Identify methods of preventing FWA;
- Identify how to report FWA; and
- Recognize how to correct FWA.

Where Do I Fit In?

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

- Sponsor (Medicare Advantage Organizations [MAOs] and Prescription Drug Plans [PDPs]);
- First-tier entity (Examples: Pharmacy Benefit Management (PBM), hospital or health care facility, provider group, doctor office, clinical laboratory, customer service provider, claims processing and adjudication company, a company that handles enrollment, disenrollment, and membership functions, and contracted sales agent);
- Downstream entity (Examples: pharmacies, doctor office, firms providing agent/broker services, marketing firms, and call centers); or
- Related entity (Examples: Entity with common ownership or control of a Sponsor, health promotion provider, or SilverSneakers®).

ACRONYM	Meaning
FWA	Fraud, Waste and Abuse

MemorialCare™

I am an employee of a Part C Plan Sponsor or an employee of a Part C Plan Sponsor's first-tier or downstream entity

The Part C Plan Sponsor is a CMS Contractor. Part C Plan Sponsors may enter into contracts with FDRs. This stakeholder relationship flow chart shows examples of functions that relate to the Sponsor's Medicare Part C contracts. First Tier and related entities of the Medicare Part C Plan Sponsor may contract with downstream entities to fulfill their contractual obligations to the Sponsor.

Examples of first tier entities may be independent practices, call centers, health services/hospital groups, fulfillment vendors, field marketing organizations, and credentialing organizations. If the first tier entity is an independent practice, then a provider could be a downstream entity. If the first tier entity is a health service/hospital group, then radiology, hospital, or mental health facilities may be the downstream entity. If the first tier entity is a field marketing organization, then agents may be the downstream entity. Downstream entities may contract with other downstream entities. Hospitals and mental health facilities may contract with providers.

I am an employee of a Part D Plan Sponsor or an employee of a Part D Plan Sponsor's first-tier or downstream entity

The Part D Plan Sponsor is a CMS Contractor. Part D Plan Sponsors may enter into contracts with FDRs. This stakeholder relationship flow chart shows examples of functions that relate to the Sponsor's Medicare Part D contracts. First Tier and related entities of the Part D Plan Sponsor may contract with downstream entities to fulfill their contractual obligations to the Sponsor.

Examples of first tier entities include call centers, PBMs, and field marketing organizations. If the first tier entity is a PBM, then the pharmacy, marketing firm, quality assurance firm, and claims processing firm could be downstream entities. If the first tier entity is a field marketing organization, then agents could be a downstream entity.

ACRONYM	Meaning
CMS	Centers for Medicaid and Medicare Services

MemorialCare

What Are Your 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 that you may be aware of.
- **THIRD,** you have a duty to follow your organization's Code of Conduct that articulates your and your organization's commitment to standards of conduct and ethical rules of behavior.

How Do You Prevent FWA?

- Look for suspicious activity;
- Conduct yourself in an ethical manner;
- Ensure accurate and timely data/billing;
- Ensure you coordinate with other payers;
- Keep up to date with FWA policies and procedures, standards of conduct, laws, regulations, and the CMS guidance; and
- Verify all information provided to you.

ACRONYM	Meaning
CMS	Centers for Medicaid and Medicare Services

MemorialCare™

LESSON 2

Stay Informed About Policies and Procedures

Familiarize yourself with your entity's policies and procedures.

Every Sponsor and First-Tier, Downstream, and Related Entity (FDR) must have policies and procedures that address FWA. These procedures should help you detect, prevent, report, and correct FWA.

Standards of Conduct should describe the Sponsor's expectations that:

- All employees conduct themselves in an ethical manner;
- Appropriate mechanisms are in place for anyone to report non-compliance and potential FWA; and
- Reported issues will be addressed and corrected.

Standards of Conduct communicate to employees and FDRs that compliance is everyone's responsibility, from the top of the organization to the bottom.

Report FWA

Everyone must report suspected instances of FWA. Your Sponsor's Code of Conduct should clearly state this obligation. Sponsors may not retaliate against you for making a good faith effort in reporting.

Do not be concerned about whether it is fraud, waste, or abuse. Just report any concerns to your compliance department or your Sponsor's compliance department. Your Sponsor's compliance department area will investigate and make the proper determination. Often, Sponsors have a Special Investigations Unit (SIU) dedicated to investigating FWA. They may also maintain an FWA Hotline.

Every Sponsor must have a mechanism for reporting potential FWA by employees and FDRs. Each Sponsor must accept anonymous reports and cannot retaliate against you for reporting. Review your organization's materials for the ways to report FWA.

When in doubt, call your Compliance Department or FWA Hotline.

ACRONYM	Meaning
FDRs	First-Tier, Downstream, and Related Entities

MemorialCare™

Reporting FWA Outside Your Organization

If warranted, Sponsors and FDRs must report potentially fraudulent conduct to Government authorities, such as the Office of Inspector General (OIG), the Department of Justice (DOJ), 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.

Details to Include When Reporting FWA

When reporting suspected FWA, you should include:

- Contact information for the source of the information, suspects, and witnesses;
- Details of the alleged FWA;
- Identification of the specific Medicare rules allegedly violated; and
- 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) or TTY 1-800-377-4950
- Fax: 1-800-223-8164
- Email: HHSTips@oig.hhs.gov
- Online: https://forms.oig.hhs.gov/hotlineoperations/index.aspx

For Medicare Parts C and D:

- National Benefit Integrity Medicare Drug Integrity Contractor (NBI MEDIC) at 1-877-7SafeRx (1-877-772-3379)

For all other Federal health care programs:

- CMS Hotline at 1-800-MEDICARE (1-800-633-4227) or TTY 1-877-486-2048

HHS and U.S. Department of Justice (DOJ):
https://www.stopmedicarefraud.gov

ACRONYM	Meaning
OIG	Office of Inspector General

MemorialCare™

LESSON 2 -Correction

Once fraud, waste, or abuse has been detected, it must be promptly corrected. Correcting the problem saves the Government money and ensures you are in compliance with CMS requirements.

Develop a plan to correct the issue. Consult your organization's compliance officer to find out the process for the corrective action plan development. The actual plan is going to vary, depending on the specific circumstances. In general:

- Design the corrective action to correct the underlying problem that results in FWA program violations and to prevent future non-compliance;
- Tailor the corrective action to address the particular FWA, problem, or deficiency identified. Include timeframes for specific actions;
- Document corrective actions addressing non-compliance or FWA committed by a Sponsor's employee or FDR's employee and include consequences for failure to satisfactorily complete the corrective action; and
- Once started, continuously monitor corrective actions to ensure they are effective.

Corrective Action Examples

Corrective actions may include:

- Adopting new prepayment edits or document review requirements;
- Conducting mandated training;
- Providing educational materials;
- Revising policies or procedures;
- Sending warning letters;
- Taking disciplinary action, such as suspension Of marketing, enrollment, or payment; or
- Terminating an employee or provider.

LESSON 2 PAGE 10 -Indicators of Potential FWA

Now that you know about your role in preventing, reporting, and correcting FWA, let's review some key indicators to help you recognize the signs of someone committing FWA.

The following pages present issues that may be potential FWA. Each page provides questions to ask yourself about different areas, depending on your role as an employee of a Sponsor, pharmacy, or other entity involved in the delivery of Medicare Parts C and D benefits to enrollees.

MemorialCare™

Key Indicators: Potential Beneficiary Issues

- Does the prescription, medical record, or laboratory test look altered or possibly 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: Potential Provider Issues

- 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: Potential Pharmacy Issues

- Are drugs being diverted (drugs meant for nursing homes, hospice, and other entities being sent elsewhere)?
- Are the dispensed drugs expired, fake, diluted, or illegal?
- Are generic drugs provided when the prescription requires 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 prescription cannot be filled (no additional dispensing fees for split prescriptions)?
- Do you see prescriptions being altered (changing quantities or Dispense As Written)?

MemorialCare™

ACRONYM	TITLE TEXT
PBMs	*Pharmacy Benefit Managers*

Key Indicators: Potential Wholesaler Issues

- 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?

Potential Manufacturer Issues

- 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: Potential Sponsor Issues

- 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?

Lesson 2 Summary

- As a person who provides health or administrative services to a Medicare Parts C or D enrollee, you play a vital role in preventing FWA. Conduct yourself ethically, stay informed of your organization's policies and procedures, and keep an eye out for key indicators of potential FWA.
- Report potential FWA. Every Sponsor must have a mechanism for reporting potential FWA. Each Sponsor must be able to accept anonymous reports and cannot retaliate against you for reporting.
- Promptly correct identified FWA with an effective corrective action plan.

MemorialCare™

Lesson 2 Summary

• As a person who provides health or administrative services to a Medicare Parts C or D enrollee, you play a vital role in preventing FWA. Conduct yourself ethically, stay informed of your organization's policies and procedures, and keep an eye out for key indicators of potential FWA.
• Report potential FWA. Every Sponsor must have a mechanism for reporting potential FWA. Each Sponsor must be able to accept anonymous reports and cannot retaliate against you for reporting.
• Promptly correct identified FWA with an effective corrective action plan.

Lesson 2 Review

Now that you have completed Lesson 2, let's do a quick knowledge check. The following questions do not contribute to your overall course score in the Post-Assessment.

MemorialCare™

APPENDIX A: RESOURCES

Disclaimers

This Web-Based Training (WBT) course was current at the time it was published or uploaded onto the web. Medicare policy changes frequently so links to the source documents have been provided within the document for your reference. This WBT course was prepared as a service to the public and is not intended to grant rights or impose obligations. This WBT course may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

The Medicare Learning Network® (MLN)

The Medicare Learning Network®, MLN Connects®, and MLN Matters® are registered trademarks of the U.S. Department of Health & Human Services (HHS).

Glossary

For the Centers for Medicare & Medicaid Services (CMS) Glossary, visit https://www.cms.gov/apps/glossary on the CMS website.

ACRONYM	TITLE TEXT
MLN	*Medicare Learning Network®,*
WBT	*Web-Based Training*
CMS	Centers for Medicaid and Medicare Services

MemorialCare™

In Closing…

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.

MemorialCare™

Congratulations!

You have completed MemorialCare's 2021 Annual Compliance Training.

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

MemorialCare™