2026 FMOL Health and HLN Compliance Education

Safeguarding Our Ministry Compliance and Privacy Program

Table of Contents

FMOL Health
Compliance Program

Our Commitment

1. Safeguarding our ministry is everyone’s role.
2. Patient and personal data is sacred to us. We will do everything we can to protect it.
3. We are called to conduct business with the utmost integrity, and we hold ourselves to the highest standards.
4. We encourage team members to report issues without fear.
5. Our aim is to prevent all unethical or illegal activities through developing and following safe and secure processes.
6. We will act swiftly to correct anything that does not meet our high standards

Code of Conduct

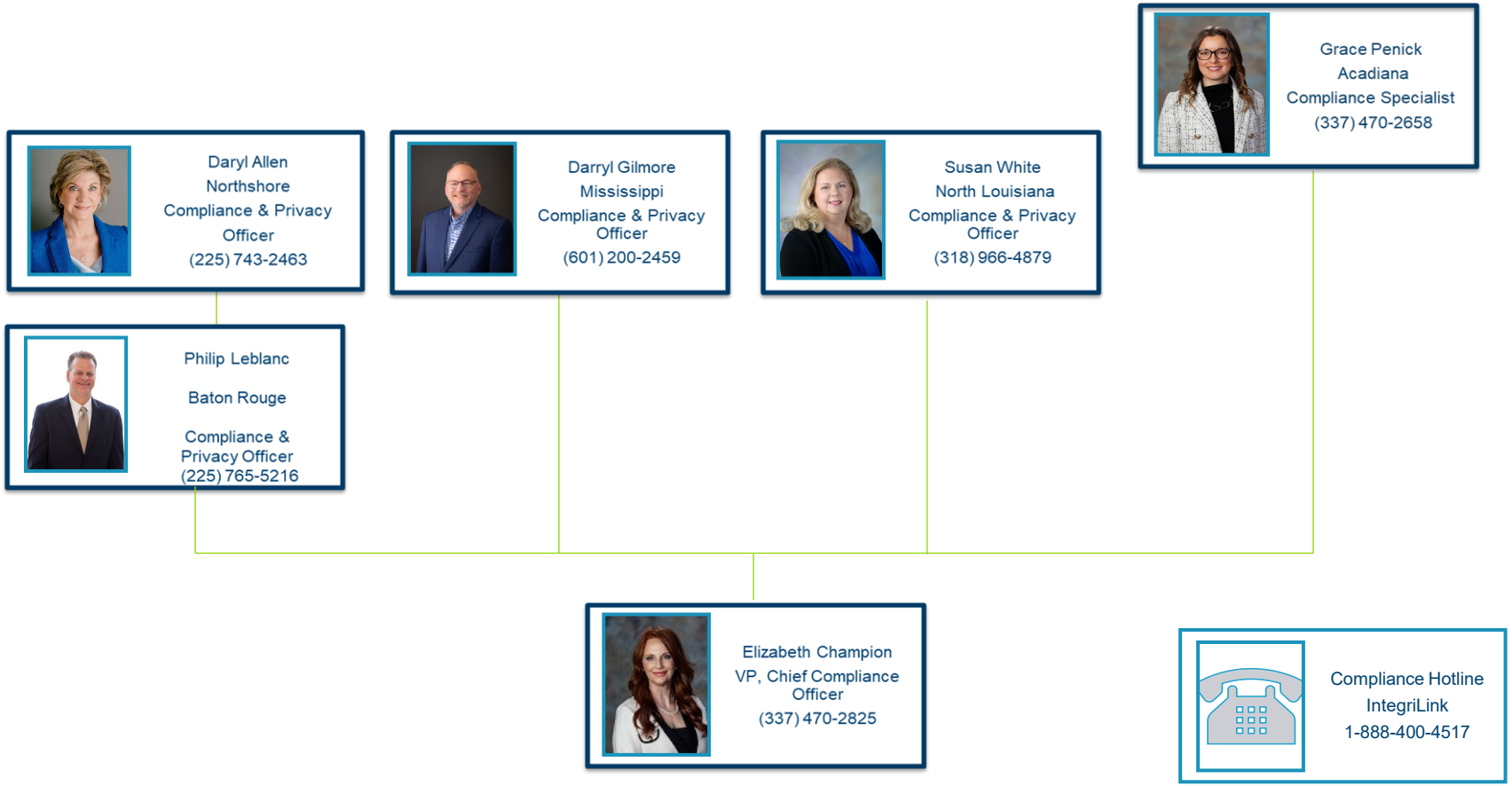
As a catholic, mission-driven organization, FMOL Health has a clear sense of our organizational ethics. Our mission, vision and values-based Compliance Program is a vital part of how we conduct ourselves in carrying out our daily activities.

Establishes expectations and responsibilities to protect information, report concerns, provide quality care and maintain honest, respectful relationships with each other, our patients and our physicians.

Requires ethical and honest behavior by avoiding conflicts of interest, disclosing conflicts when they arise and making business decisions, without personal bias, with the best interest of FMOL Health in mind.

Supports our pledge to follow all applicable rules and regulations.

FMOL Health Compliance Leadership



Compliance Program Elements

The Health Leaders Network Compliance program is based on the seven elements defined by the Department of Health and Human Services Office of Inspector General as the framework for healthcare providers to work within. The elements are as follows:

1. High Level Oversight
2. Standards of Conduct/Policies and Procedures
3. Open Lines of Communication/Reporting
4. Response to detected deficiencies
5. Education and Training
6. Monitoring and Auditing/Risk Assessment
7. Consistent Enforcement Standards

Ongoing Compliance Activities

- The Compliance program monitors procedures to ensure that the ACO participants and providers:

Meet the exclusion screening requirements of the ACO participation agreements.

Receive the training necessary to comply with regulations, and complete all attestations, affirming the ACO practice and participating providers comprehend the material.

Adhere to all corrective action plans, remedial processes, and sanctions to improve compliance and performance.

Comply with the FMOL Health compliance plan to ensure that all probable violations of law are reported to law enforcement.

Communicate routinely with the FMOL Health and HLN Board and participate in quality reporting.

Conflict of Interest

What is Conflict of Interest?

A **conflict of interest** is any situation that does or looks like a team member is putting personal interest ahead of what is good for FMOL Health

- Includes family members and friends
- Team members must make decisions and do their work in a way that supports FMOL Health
- Team members must not use their position, responsibilities or knowledge for personal gain

Who must follow it?

Everyone

Where to report Issues?

Actual or potential conflicts of interest should be reported to the Compliance Officer.

1. Contact your local Compliance Officer
2. Connect to fmolhsintegritylink.com
3. Call the anonymous hotline 888-400-4517

Physical Security

1

Protecting Physical Assets

Keep all physical assets safe.
Examples:

1. ID badges
2. Lock doors and set alarms
3. Lock file cabinets and desks
4. Use surveillance cameras
5. Security officers
6. Electronic Devices
   - Turn computer screens away from public view or use a privacy screen
   - Keep laptops or devices in a secure place
   - NEVER connect a device to our network that is not issued to you by FMOL Health. –If you didn't get it from IS, then don't use it!

2

Dispose Materials Properly

- Shred bins are located on every floor. Shred all sensitive materials.
- Do not throw sensitive information in the trash can.
- Shred all sensitive information – IV Bag labels, cards, labels, arm bands
- Mobile devices that access PHI must have passwords in place for access.
- Cell phones, iPads, laptops, thumb drives, USB drives, DVDs, etc. should not have any sensitive information without having a password or encryption on the media. This will prevent the information from being lost if stolen.

3

Transporting Documents/ Equipment

- Don't take WOWs, carts or handheld devices away from the hospital
- All equipment or documents should remain onsite at FMOL Health unless your job requires you to take it.
- If you access information at home, be sure family or friends cannot view the information.
- Never leave devices unattended.
- If transporting information:
  - Paper documents should be in a sealed envelope
  - Never leave laptop or devices in the car
  - If you must make a stop, take the information with you.

Password Security

- You are responsible for keeping your password secure.
  - NEVER share your password with anyone. This includes your office staff and the IS Support Center or anyone in IS.
  - Create computer passwords that meet the FMOL Health password criteria. Example: Tm2tbg# (Take me to the ball game)
  - Keep your password in a secure manner. DO NOT write your password down. Commit it to memory.
  - Change your password when prompted or at least every 180 days.
  - DO NOT use shared logins to access an application
  - Everyone should have their own login to all

Securing PHI Data

1

Never save or share PHI on public Internet or Cloud service

- Examples include Dropbox, Apple iCloud, Google Docs

2

When you do receive patient population data, save wisely:

- Never save protected or confidential PHI to your local hard drive or a personal or non-work computer
- Save patient data to applications/sources of record (e.g.,, Epic, PACS, Cerner)
- Save other data to network drives/shares only as appropriate
- Only store confidential data on authorized devices
- Desktops, laptop computers, and USB devices are not meant for permanent data storage
- Regularly back-up your data, preferably to a network drive/share

3

Never email confidential data (ePHI) to a personal email account

- Examples: Gmail, Yahoo, Hotmail, Comcast, MSN

Email Security

1

Secured Email

E-mail sent to people outside of FMOLHS is like a postcard that can be read by others along the way – it is not secure unless you type ‘Secure’ in the subject line.

2

External Email

Do not send PHI or other sensitive information outside of FMOLHS by e-mail.

3

Email Attachments

Do not open an e-mail attachment if you have any doubts about the source. Attachments may contain a computer virus which can destroy information

4

Suspicious Emails

Call the IS Support Center if you receive a suspicious e-mail or think your computer has a virus.

Screening for Excluded Providers

1

The Federal excluded individual rule prohibits a provider from submitting a claim to Medicare for any good or service furnished by or at the direction of an excluded individual.

2

FMOL Health screens team members, Medical Staff members, contractors and vendors against governmental excluded individual organization lists.

3

If excluded providers participate in ACO and FMOL Health health care activities, the services provided and/or the ACO application could be denied, or additional program safeguards could be imposed.

4

Participants have a duty to immediately notify the FMOL Health and/or ACO of any investigations or exclusions.

Avoiding Improper Referrals

1

Providers must maintain beneficiary freedom of choice.

2

ACOs are prohibited from requiring that Participants refer within the ACO for non-ACO patients.

3

The Final Rule also prohibits ACOs from requiring that beneficiaries be referred within the ACO.

4

Improper referrals can lead to over-utilization, increased costs, corruption of medical decision making, patient steering, and unfair competition.

Federal Sentencing Guidelines

Provide **incentives** to organizations, such as reduced fines and penalties, that have effective compliance programs

Promote corporate **accountability and responsibility** and stress **"good citizenship"** by corporations

Promote a **culture of ethical behavior and values**, beyond just following the law

Expect **governance oversight** of compliance programs

Emphasize ongoing **risk assessment** as part of an effective compliance program

HIPAA Privacy and Security

Confidentiality and Privacy Requirements

1. Federal and state laws require FMOL Health Covered Entities and Health Leaders ACO to maintain the privacy and security of all patient health information (“PHI”).
2. All FMOL Health Covered Entities and Health Leaders ACO participants are required to:
   - Treat PHI as confidential in all forms – e.g., paper, electronic and verbal discussions
   - Access and use only the minimum amount of PHI necessary to perform your job
   - Take reasonable measures to protect the confidentiality and security of PHI
   - Comply with all requirements of CMS’ Data Use Agreements (“DUA”), where applicable to your role and responsibilities

Why do we need to protect PHI?

1. It’s the law
2. To protect our reputation
3. To avoid privacy breaches and potential fines
4. To build trust between providers and patients

Appropriate Access

Need to Know - Minimum Necessary

1

- “Minimum Necessary” is sharing only enough PHI as is needed in the situation
- When answering a request for information other than for treatment, ask yourself: “What is the minimum necessary information needed to meet the request?”
- The minimum necessary rule does NOT apply to requests for which the patient has given permission or for treatment

2

- Only look at PHI you need to know for your job.
- Applies to PHI in the computer and on paper
- Do not access your own, co-worker, family or friends’ health information, unless you need it for your job
- Go to HIM if you want to view your own health information
- Share PHI only with those who need to know.
- Only share PHI with team members who are involved in the patient’s care
- Discuss patient information in private places
- Close doors or pull curtains
- Do not talk about patients in public areas such as waiting rooms, hallways, elevators or the cafeteria
- Do not talk about patients outside of work
- Do not post information about patients on Facebook or other social media

3

- Limit PHI given when leaving a message for a patient with another person or on voicemail or answering machine
- Refer all requests from media to the Public Relations department
- Cover, file or put away all papers that have PHI
  - Do not leave lists, schedules or other papers with PHI in public view
  - Lock doors where PHI is stored
- Throw papers with PHI in bins for confidential waste or shred them immediately
  - Includes hand-written notes, reports, face sheets, labels
    - Black out (with a pen or marker) PHI on IV bags before throwing in the trash

Common Privacy Breaches

1. A team member views the record of a co-worker to determine why they have been out of the office

2. A RN discharging a patient gives the patient discharge instructions for a different patient

3. A CNA views the record a local celebrity that was a recent inpatient out of curiosity

4. A provider leaves a patient in an exam room to retrieve supplies but leaves himself logged into the computer. Patient views another patient's information while the provider is out of the room

5. A team member who works at Dr. Smiths Office, mentions to a friend that she saw their mutual friend at the office for an appointment

Social Media

Common Social Media HIPAA Violations

Posting comments about patients (even if their name is left out)

Posting photographs of patients or PHI without patient consent

Posting workplace photographs that accidently contain patient information

Commenting on another person's post about patients

Social Media Best Practices

1. Professional standards apply to online content
2. Understand your market's social media policy
3. Don't mix work and personal life - online contact with patients blurs this boundary
4. Never post about patients- even in general terms
5. Don't trust private messages
6. Do not take photos or videos of patients on personal devices, including cell phones
7. Consider avoiding identifying your employer on your social media profiles
8. Don't post anything online that you wouldn't say in front of your boss or human resources
9. Promptly report any identified breach of confidentiality or privacy

How do privacy concerns affect patients?

1

27% Withhold information from care provider due to privacy concerns

2

64% Leave care provider because of a breach publicized in social media

3

28% Postpone seeking care due to privacy concerns

4

85% Choose providers based on reputation for keeping patient records private

5

60% Travel to seek care elsewhere due to privacy concerns

What happens when a privacy violation occurs?

1. Following a violation, we must:
   - Investigate along with Human Resources and other leaders as appropriate
   - Perform a risk assessment to determine if a breach occurred
- When a breach occurs, we must:
   - Notify the affected patient(s) within 60 days of discovery
   - Report the breach to the Office for Civil Rights (OCR)
   - If the breach affects greater than 500 people of a state or jurisdiction, we must provide notice to the media and report the breach to the OCR simultaneously with patient notification
   - Appropriately and consistently discipline team members involved in the breach

Fraud, Waste and Abuse

Fraud, Waste & Abuse

What is Fraud?

- Deceiving someone on purpose
- Being dishonest to gain an advantage
- Getting an advantage by hiding important facts

What is Waste and Abuse?

- Improper or excessive use of Medicare or Medicaid program
- Misuse of resources
- May not be done on purpose
- Could be an error
- Happen when procedures are not checked

Fraud, Waste & Abuse Examples

- Providing “free” services and billing the insurance provider
- Unbundling services that should be billed together
- Providing medically unnecessary services
- Billing for items or services that were never done
- Double billing
- Putting another doctor's name on a bill
- Changing the date of service so insurance would pay the bill
- Incorrect coding

Penalties and Facts

Fraud, Waste & Abuse FACTS:

1. Between 3% and 10% of healthcare spending is lost due to fraud. That amounts to:
   - $67 - $230 billion lost each year
   - $184 - $630 million dollars lost each day
2. Healthcare fraud is believed to be one of the largest white-collar crimes in the US
3. Healthcare fraud is often thought to be a victimless crime, but it affects everyone

Penalties

If an organization or person is found to be in violation of Fraud, Waste, and/or Abuse laws or regulations, the penalties may be:

1. Monetary penalties or fines
2. Corporate Integrity Agreement - Required to follow the Government's compliance program
3. Not allowed to be part of the Medicare and Medicaid programs
4. Discipline up to and including termination
5. Jail sentences for employees, administrators, and physicians
6. Loss of public trust

False Claims

What is a False Claim?

- A false claim is sending an incorrect or dishonest statement to the federal or state government to get paid for services when you knew or should have known that the claim was false.
- Louisiana also has a law against sending false claims to the government called the “Medical Assistance Programs Integrity Law”. (See Policy COMP 08 001 for more information)
- The False Claims Act is a federal law and was put in place to fight and prevent fraud and abuse by providers and others that are part of medical assistance programs

Examples of False Claims

1. Overcharging for a product or service
2. Billing for services not given
3. Billing for more services than given
4. Billing for services that are not medically necessary
5. Not paying money that is owed back to the government
6. Charging for one thing, but delivering another
7. Winning a contract or patient referrals through kickbacks or bribes

Penalties

There are major penalties for submitting false claims. A company or person that has made a false claim may be subject to:

1. Three times the amount of the false claim
2. A fine of $14,308 to $28,619 per false claim
3. Not allowed to be part of federal healthcare programs (Medicare and Medicaid)
4. The attorney’s fees of a whistleblower, if there was one

Compliance with Fraud, Waste & Abuse Laws

- FMOL Health and the Health Leaders ACO is also required to abide by federal and state Fraud and abuse laws.
- These laws prohibit the payment or exchange of anything of value to induce or reward patient referrals paid by a federal or state health care program.
- FMOL Health and Health Leaders ACO and participants may not offer, solicit, pay or receive anything of value, directly or indirectly, for referring patients or furnishing or arranging for goods or services.
- All referral decisions will be based solely on the health care needs of Health Leaders ACO patients.

FMOL Health and the Health Leaders ACO is committed to honest and lawful conduct, including following all laws and regulations that apply to participation.

Whistle Blower Act

- A whistleblower is someone who knows about a false claim being made and reports it to the government.
  - A whistleblower may file a “qui tam” or whistleblower lawsuit against the company or individual.

- The Whistleblower Protection Act is a law that protects employees who report a violation or suspected violation of state, local or federal law.
  - Does not allow the employer to fire, threaten, or otherwise discriminate against an employee because the employee reports or is about to report a violation.
  - Allows for the whistleblower to receive a percentage of the recovered money if there is a settlement or judgment against the organization.

Governing Laws

Anti-Kickback Statute

1. This law says that we may not knowingly solicit, receive, offer or paying anything of value for referrals for services that are paid in whole or in part by a federal health care program, including Medicare. This means that we may not:
2. Pay patients, physicians or other healthcare providers for referrals
3. Give physicians free office staff, free rent or free services
4. Offer patients free services or other gifts to receive care from us
5. Penalties include:
6. Fine up to $100,000;
7. Imprisonment up to 10 years; or
8. Both fine and imprisonment

Stark Law

This law does not allow a physician to make a referral for certain designated health services to an entity in which the physician (or a member of his or her family) has an ownership or investment interest. Hospitals may not bill for services provided based on those referrals.

Penalties include:

1. Up to a $15,000 fine for each service provided
2. Up to a $100,000 fine for entering an improper arrangement
3. FMOLHS has procedures in place to be in compliance with the Stark Law.

Deficit Reduction Act of 2005 (DRA)

The federal government requires healthcare providers to have compliance program for all providers or organizations that receive over $5 Million in Medicaid payments a year

The Sunshine Act

- The Sunshine Act requires drug and device companies to collect and annually report data to CMS on payments, gifts and other transfers of value to physicians and teaching hospitals. CMS posts this data on a public website www.cms.gov/openpayments.

- Manufacturers and group purchasing organizations (GPOs) are also required to disclose physician ownership and investment interests to CMS for reporting.

- Physicians are allowed at least 45 days to review and correct reported information prior to publication, if they are registered in the database. Physician registration is voluntary.

The Sunshine Act

Q: What is being reported?

A: Payments, transfers of items that have value, and ownership interests. Manufacturers must specify the nature of the payment or transfer of value and are required to report on ownership interests held by physicians and their immediate family members. The transparency report must include the dollar amount invested, the value, and terms of ownership or investment interest, and any payment provided to physician owner or investor. The reports are published by CMS on June 30th of each year.

Q: What is exempt from reporting?

A: Samples are exempt as long as they are provided to patients. Educational materials that benefit patients are exempt. Meals will not be exempt (unless under $10), but meals will count regardless if the total in a reporting year cumulatively is valued at $100 or more. Also, any payment or transfers of value are subject to reporting.

Other Governing Laws

Emergency Medical Treatment and Active Labor Act (EMTALA)

1. EMTALA is a federal law and requires hospitals and urgent care clinics to provide appropriate medical screening to anyone who comes to the site and needs treatment for an emergency medical condition – **even if they cannot pay**.
2. This includes any patient, visitor or team member who has a medical need (fall, seizure, etc.) on hospital property.
3. For an emergency condition or active labor, we must:
   - Provide and document a medical screening exam
   - Stabilize the patient, if possible
   - Provide treatment
   - Transfer the patient to an appropriate facility if we cannot provide the needed treatment

Requirements

Accurate Books and Records

Team members must report honest and accurate information on all documents including:

1. Timecards
2. Financial reports
3. Expense reports
4. Patient accounts and bills
5. Medical records

This helps us:

1. Maintain integrity
2. Have accurate information to provide high quality care
3. Support charges for our services
4. Follow laws and regulations that involve these types of records

Exclusion from Federal Health Care Programs

Federal health care program payments may not be made for any item or service furnished, ordered or prescribed by an individual or entity excluded by the Office of Inspector General. Excluded individuals may not be employed by or contract with FMOL Health.

To assure compliance, FMOL Health:

1. Screens all new employees upon hire and then on a monthly basis
2. Screens all physicians when joining the medical staff and then on a monthly basis
3. Screens all vendors on a monthly basis

Reporting Compliance Concerns

How You Can Help Safeguard Our Ministry

- Patient privacy is sacred to us. Honor your commitment to our patients and to the Ministry to always protect patient information.
- If you see something, say something. Report, in good faith, all concerns.
- Only access information you need to complete your job duties.
- When you are a patient or have a family member who is a patient, you must access information through MyChart and/or HIM after presenting appropriate authorization.
- Do not access information in Epic or other systems containing PHI for personal reasons.
- Do not look up room numbers for hospitalized co-workers you are not caring for, through your work queues, lists, snapshots or other report containing PHI. This access allows the viewer to see information that should be accessible to care team members only.

CMS ACO Requirements

ACO Compliance Requirements

CMS has established specific compliance requirements for ACOs that go beyond those that otherwise apply to health care providers including:

1. Medically Necessary and Appropriate Care
2. At-Risk Beneficiaries
3. Beneficiary choice
4. Beneficiary notices
5. Communications with beneficiaries
6. Beneficiaries Gifts
7. Other requirements

Medically Necessary and Appropriate Care

Health Leaders ACO is committed to achieving the goals of:	Medicare ACOs may not:
Better health and care	Deny, reduce or limit medically necessary services.
Lower costs	Over-utilize services provided to non-ACO beneficiaries to offset reduced ACO revenues
Providing medically necessary and appropriate care	Condition participation in the ACO on referrals of non-ACO business.

At-Risk Beneficiaries

- Medicare ACOs may not avoid beneficiaries with high-cost medical needs.
- An "at-risk" beneficiary is a patient who:
  1. has a CMS high risk score;
  2. has one or more chronic conditions;
  3. is dually eligible for Medicare and Medicaid;
  4. is diagnosed with a mental health or substance abuse disorder;
  5. has had a recent diagnosis that is expected to result in increased cost;
  6. has had two or more hospitalizations or emergency room visits each year;
  7. or otherwise has a high health care utilization pattern.
- The ACO may identify at-risk beneficiaries to better coordinate and deliver care more efficiently.

Beneficiary Choice

- No – Health Leaders ACO is not a managed care plan or a closed network program.
    1. Medicare fee-for-service beneficiaries are free to seek care from providers outside of the ACO.
    2. Health Leaders ACO participants may not engage in practices or adopt policies that restrict or limit the right of Medicare fee-for-service beneficiaries to obtain health care services from providers they choose.

Beneficiary Notice

- CMS has established requirements for how ACOs should notify beneficiaries about changing their option to decline the sharing of their health care information.

- Three Ways Beneficiaries Are Notified of Their Option to Decline Sharing Their Health Care Information
  - Advance notice through CMS materials.
  - A sign/poster on display always in ACO participant facilities
  - A written notice available upon request, at the point of care.

- Beneficiaries must contact 1-800-MEDICARE to decline sharing their information or to reverse that decision.

Communications with Beneficiaries

- **Are there other ACO requirements for communications with Medicare beneficiaries?** Yes – CMS has placed significant limitations on ACO communications (also referred to as “marketing materials,” “marketing activities,” and “marketing events”) with Medicare beneficiaries:
- **What are Marketing Materials?** Marketing materials are materials created for the general audience and used to educate, notify, or contact beneficiaries regarding the ACO’s participation in the ACO Model.

“Marketing Materials” include	“Marketing Materials” do not include
Beneficiary notices	Billing and claims information
Brochures	Materials on other specific individual health related issues
Websites	Educational materials on health care conditions
Advertisements	Materials customized or limited to a subset of beneficiaries
Data sharing opt out letters	Materials that do not contain information about the ACO or ACO providers
Outreach events	Written referrals for health care services
Mailings	
Social media	

Communication with Beneficiaries (cont'd)

- **What are marketing materials?** Marketing activities are the distribution of marketing materials to educate, notify, or contact beneficiaries regarding the ACO's participation in the ACO Model.

  These activities can include activities related to voluntary alignment (VA). These activities may be conducted by, or on behalf of, the ACO and its providers.

- **What is Voluntary Alignment?** Voluntary Alignment is the process in which beneficiaries may choose to align to an ACO voluntarily. The beneficiary designates an ACO participant provider as their primary care provider or main source of care. A beneficiary who indicates that a Participant Provider is his or her primary clinician or main source of care generally will be aligned to the ACO, even if the beneficiary would not otherwise be aligned to the ACO based on claims-based alignment.

  There are two ways for a beneficiary to be voluntarily aligned to an ACO—Medicare.gov and Signed-Attestation Based voluntary alignment.

Note: All marketing, communications, and outreach materials or events related to voluntary alignment require approval from CMS prior to use.

Communications with Beneficiaries (cont'd)

- **Regulations for Beneficiary Education about Voluntary Alignment:**

CAN:	CANNOT:
Answer beneficiary questions about Voluntary Alignment.	Complete a Voluntary Alignment form on behalf of the beneficiary.
Instruct beneficiaries to call the ACO for questions about Voluntary Alignment.	Designate a primary clinician on MyMedicare.gov (or any successor site) on behalf of the beneficiary.
Provide beneficiaries with information about the ACO and VA IF that information has been approved by both the ACO and CMS.	Include the Voluntary Alignment form and instructions with any other materials or forms, such as materials requiring the signature of the beneficiary.
	Withhold or threaten to withhold medical services or limit or threaten to limit access to care.

Communication with Beneficiaries (cont'd)

What are Marketing Events? Marketing events are one type of marketing activity designed to educate beneficiaries about the ACO's participation in the ACO Model.

In conducting marketing events, the ACO may engage in activities including, but not limited to:

- Hosting the marketing event in a public venue;
- Answering beneficiary-initiated questions regarding the ACO's participation in the Model; and/or
- Distributing the ACO's, a Participant Provider's, or a Preferred Provider's business cards and contact information to beneficiaries.

The following are prohibited as part of any marketing events:

- Health screenings or any other activity that could be perceived as or used to avoid treating at-risk beneficiaries or to target certain beneficiaries for services for the purpose of trying to affect alignment to the ACO for a future Performance Year.
- Requiring attendees to provide their contact information as a prerequisite for attending the marketing event; any sign-in sheets used for purposes of the marketing event must be clearly labeled as optional.

Communication with Beneficiaries (cont'd)

1. All ACO marketing materials, activities, and events for actual or potential Medicare beneficiaries require advance approval by CMS.
2. ACOs are prohibited from using incorrect or misleading information in marketing materials.
3. ACOs may not modify template marketing materials provided by CMS without approval of CMS.
4. ACOs may not use marketing materials or conduct marketing activities through the use of door-to-door solicitation, approaching beneficiaries in common areas, or using telephonic solicitation.
5. ACOs may not conduct marketing activities in restricted areas of a health care setting including exam rooms, hospital patient rooms, treatment areas, and pharmacy counter areas.
6. Medicare and ACO contact information must be included in all materials developed or distributed to Medicare beneficiaries.
7. CMS prohibits the use of certain specific language, phrases and terms in ACO marketing materials.

Prohibited	CMS Suggested Alternative
"Managed care" or "care management"	"Coordinated care" or "care coordination"
Beneficiaries "enroll" or "enrollment"	Providers "participate"
"You have been selected to participate"	"Your provider has chosen to participate"

Communication with Beneficiaries (cont'd)

ACO marketing activity and material cannot:

- Suggest beneficiaries are required to see only ACO providers or are in any way prohibited from seeing providers outside the ACO.
- Suggest beneficiaries enroll or are participating in ACOs; it is the provider, not the beneficiary, that has chosen to participate in the ACO.
- Suggest CMS endorses one ACO over another.
- Suggest an ACO is in any way superior to other ACOs, or other types of ACOs, or that providers participating in the ACO are superior to other providers participating in other ACOs or CMS initiatives.

Beneficiaries Gifts

Can an ACO offer free or discounted services to Medicare beneficiaries?
Yes – but strict limitations apply.

ACOs are allowed to provide Medicare beneficiaries free or below market value items and services to encourage care coordination and beneficiary health awareness when it meets all of the following requirements :

1. "In-kind" (e.g., goods, commodities, and services, but not cash);
2. Reasonably connected to the medical care of the beneficiary; and
3. Either preventive care items or services or intended to advance one or more of the following clinical goals:
   - Adherence to a treatment regime
   - Adherence to a follow-up care plan; and/or
   - Management of a chronic disease or condition

Beneficiaries Gifts (cont'd)

ACOs may not give Medicare beneficiaries:

- Cash or items unrelated to health care under any circumstances (e.g., sporting event tickets, gift certificates for non-health care items)
- Items or services as a reward for receiving services from the ACO
- Items or services to persuade a Medicare beneficiary to remain in the ACO or with a particular ACO provider

Appropriate	Inappropriate
An ACO may provide a blood pressure monitor to a patient with hypertension to encourage regular blood pressure monitoring Beneficiary notices	An ACO may not waive or reduce Medicare copayments or deductibles unless based on a beneficiary's financial need. This would be considered a financial incentive, not "in-kind" goods and services

Other Requirements

Health Leaders ACO must also adhere to additional requirements of the ACO Program including:

1. Development of processes supporting evidence-based medicine, quality assurance, and patient engagement
2. Periodic submission of quality data, certifications and other information in accordance with CMS requirements
3. Retention of all records related to the ACO for a minimum of 10 years after the ACO agreement period ends

All Health Leaders ACO participants are expected to cooperate in the gathering, recording and submitting of data in a timely, accurate and complete manner and in assist in meeting all other requirements.