



CODE OF ETHICAL BUSINESS
CONDUCT AND COMPLIANCE

First Tier, Downstream, and Related Entities



Dear Valued Partner:

Our reputation of high standards for business integrity and ethical business conduct is one of our most valuable assets in our partnership with you. We are strongly committed to legal and ethical conduct as an integral part of the operation of our business.

University of Maryland Health Advantage, Inc. is focused on conducting its business operations in compliance with all applicable federal, state, and local laws, and applicable government health care program requirements. But even more importantly we are committed to conducting ourselves at all times with integrity.

Our core values guide our behaviors and are rooted in our success.

- Service to our Members
- Respect
- Excellence
- Integrity
- Teamwork

Our reputation and success is not only dependent upon our conduct, but also on the conduct and judgment of the individuals and organizations on whom we rely for products and services that support our organization's purposes. University of Maryland Health Advantage, Inc. has chosen to do business with you because we believe there is a shared commitment to professional and ethical business conduct and practices.

We have zero tolerance for unethical, non-compliant, and criminal conduct by our Associates, Board of Directors, First Tier, Downstream, and Related Entities, and individuals with whom we conduct business. Always remember that what you do matters, regardless of your role with University of Maryland Health Advantage, Inc. As First Tier, Downstream or Related Entity you have the opportunity every day to promote and support an ethical culture by serving all customers with integrity, respecting co-workers, seeking guidance and bringing forth concerns without fear.

We have prepared this Code of Ethical Business Conduct and Compliance for First Tier, Downstream and Related Entities to guide you in making good ethical decisions and complying with applicable federal, state, and local laws, and applicable government health care program requirements.

We thank you for your partnership with us.

Sincerely,

Mark Puente
President and Chief Executive Officer,
University of Maryland Health Advantage, Inc.



Know your Compliance ABC's

Table of Contents

University of Maryland Health Advantage Inc.'s Medicare Compliance Program & Code of Ethical Business Conduct and Compliance for First Tier, Downstream and Related Entities	4
What's a FDR?	5
Medicare Compliance Program and Attestation Requirements.....	6
Compliance program requirements.....	6
What may happen if you don't comply	7
Attestation requirements.....	7
You may be asked to provide evidence of compliance	7
Fraud, Waste and Abuse ("FWA") training, General Compliance training and Code of Conduct/Compliance policy distribution.....	8
FWA and general compliance training	8
Compliance training requirements	8
You must give your employees this Code of Ethical Business Conduct and Compliance for FDRs.....	8
Exclusion list screenings	9
You must perform exclusion list screenings	9
You must take action if an employee or Downstream Entity is on the list.....	9
Reporting Violations to University of Maryland Health Advantage, Inc.	10
Medicare Compliance Officer	10
Non-Retaliation Policy	10
Your Obligation to Cooperate in Investigations	11
Offshore operations & CMS reporting	11
Notify us immediately if you plan to use an Offshore Entity.....	11
Model of Care Training	11
Specific federal and state compliance obligations	12
Monitoring and auditing of First Tier and Downstream Entities.....	12
Expect routine monitoring and audits	12
University of Maryland Health Advantage's Workplace Standards and Practices	13
Workplace Violence	13
Weapons.....	13
Smoke-Free Workplace	13
Drug-Free Workplace	13
Health, Safety, and Environment	13
Solicitation, Distribution of Materials and Bulletin Boards.....	13
Communications and Distribution	14
Communications and Public Affairs	14
FDR Relationships with Company Employees.....	15

Confidential and Proprietary Information 15
University of Maryland Health Advantage, Inc. Electronic Assets..... 15
University of Maryland Health Advantage, Inc. Records, Record Retention and Destruction..... 16
Passwords and Access Codes 16
Security Requirements..... 16
Questions/Concerns 17



University of Maryland Health Advantage Inc.'s Medicare Compliance Program & Code of Ethical Business Conduct and Compliance for First Tier, Downstream and Related Entities

University of Maryland Health Advantage Inc.'s (hereinafter referred to as "Company") reputation depends on our ability to deliver on our promises to our members and our network of physicians, providers and facilities. We are guided by the highest standards of integrity. Our relationships with our members, providers, business partners and suppliers are built on trust and through experience. Each day we must deliver our commitment to do the right thing for the right reason and keep the people we serve at the center of everything we do.

Our Medicare Compliance Program helps us serve our members ethically

We're committed to practicing business in an ethical manner. Our Medicare Compliance Program is designed to:

- Reduce or eliminate fraud, waste, and abuse
- Make sure we comply with applicable laws, rules and regulations
- Reinforce our commitment to compliance

We use external entities to bring our members cost-effective healthcare solutions

The Company offers a Medicare Advantage Prescription Drug Plan and a Dual Special Needs Plan (collectively, "Medicare Plans"). We contract with several external individuals and entities as a cost effective and efficient way of providing administrative and healthcare services. Some of the services provided by external entities are services that we are required to perform under our contracts with CMS. The Centers for Medicare and Medicaid Services (CMS) refer to these entities as First Tier, Downstream, and Related entities (FDRs).

You'll find specific requirements in this document

CMS also requires that the Company's FDRs fulfill specific Medicare Compliance Program requirements. We describe these requirements in this document. The Code of Federal Regulations (CFR) outlines these Medicare Compliance Program requirements and they are specifically defined by CMS in the January 11, 2013 release of the Compliance Program Guidelines found in Chapter 21 of the [Medicare Managed Care Manual](#) and Chapter 9 of the [Prescription Drug Benefit Manual](#) (Manual), which are identical.

It is important for you to follow these requirements

You received this Code of Ethical Business Conduct and Compliance for First Tier, Downstream and Related Entities (hereinafter referred to as "the Code") because we've identified you as a FDR. This means that you must comply with these requirements. You must ensure that any employees and downstream entities who are assigned to work on Company Medicare business adhere to the Code and all laws, rules and government regulations applicable to Company whenever they are conducting business for and/or on behalf of Company.

FDRs will exercise appropriate supervision and oversight of their employees and downstream entities to make sure that they are adhering to all Company training requirements and that any work performed for or on behalf of Company is consistent with the Code. The Company will require FDRs to demonstrate that they are in compliance with the Code.



The Code establishes minimum standards for conducting business with Company and to the extent of any conflict between the Code and any other transactional document entered into by Company and you, the latter will control.

What's a FDR?

We use the current CMS definitions to define First Tier, Downstream, and Related Entities:

First Tier Entity is any party that enters into a written arrangement, acceptable to CMS, with a Medicare Advantage Organization or Part D plan sponsor or applicant to provide administrative services or healthcare services to a Medicare eligible individual under the Medicare Advantage program or Part D program. (See, 42 C.F.R. §§ 422.500 & 423.501).

Downstream Entity is any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the Medicare Advantage benefit or Part D benefit, below the level of the arrangement between a Medicare Advantage Organization or applicant or a Part D plan sponsor or applicant and a first tier entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services. (See, 42 C.F.R. §§ 422.500 & 423.501).

Related Entity means any entity that is related to a Medicare Advantage Organization or Part D sponsor by common ownership or control and :

Performs some of the Medicare Advantage Organization or Part D plan Sponsor's management functions under contract or delegation; or,

Furnishes services to Medicare enrollees under an oral or written agreement; or,

Leases real property or sells materials to the Medicare Advantage Organization or Part D plan Sponsor at a cost of more than \$2,500 during a contract period.

(See, 42 C.F.R. §§ 422.500 & 423.501).

FDRs providing healthcare services

The Medicare Compliance Program requirements described in the Code applies to healthcare providers contracted with Company to participate in our Medicare Plan network. This includes physicians, hospitals and other provider types. Here are the reasons why:

- First, Medicare Advantage (MA) regulations and CMS rules clearly state that providers contracted with The Company to provide healthcare services to our Medicare members are "First Tier Entities."
- Second, Chapters 9 and 21 of the Manual lists "healthcare services" as an example of the types of functions that a third party can perform that relates to an MA organization's contract with CMS. This would give third parties "First Tier Entity" status. (See last bullet point in the Manual, Chapters 9 & 21 § 40.) So, these Medicare Compliance Program requirements apply to providers that actually deliver healthcare services to our Medicare members.
- Third, CMS provides a chart in the Manual, Chapters 9 & 21 § 40 showing that entities providing health services and hospital groups are first tier entities. So, if we contract with a hospital group and don't have direct contracts with the group's hospitals and other providers, the hospitals and providers are "Downstream Entities." This means that the hospital group is a "First Tier Entity,"



and must comply and make sure its Downstream Entities comply with the CMS compliance program requirements in this guide.

FDRs providing administrative services

The Medicare Compliance Program requirements also apply to entities with which we contract to perform administrative service functions relating to our Medicare Advantage contract with CMS. Some examples of administrative service functions include, but are not limited to:

- Formulary Administration
- Part D Claims Processing
- Behavioral Health Claims Processing
- Behavioral Health Utilization Management
- Coverage Determinations
- Medical Record Reviews
- Disease Management
- Case Management
- Translation Services
- Credentialing*

*Under our Medicare Advantage contract with CMS, we're required to credential healthcare providers that participate in our Medicare Plan network. We contract with entities to perform these credentialing services on our behalf under a delegation agreement. CMS considers these delegated credentialing entities to be First Tier Entities. CMS identifies delegated credentialing entities as First Tier Entities in the Manual, Chapter 11 § 100.5.

Other examples of FDRs include delegates, agents, broker organizations, pharmacies and other individuals, entities, vendors or suppliers contracted with The Company to provide administrative and/or healthcare services for our Medicare Plans. You can find more information in CMS Medicare Managed Care and Prescription Drug Manuals, Chapters 9 & 21.

Medicare Compliance Program and Attestation Requirements

It's important that our FDRs are in compliance with applicable laws, rules and regulations. Although we contract with FDRs to provide administrative and/or healthcare or prescription drug services for our Medicare Plans, in the end, we're responsible for fulfilling the terms and conditions of our contract with CMS and meeting applicable Medicare program requirements.

Compliance program requirements

First Tier Entities are responsible for making sure that their Downstream Entities comply with applicable laws and regulations, including the requirements in this guide. As a First Tier Entity, you/your organization and all of your Downstream Entities (if applicable) must comply with Medicare Compliance Program requirements. The Code summarizes your Medicare Compliance Program responsibilities. Please review it to make sure that you have internal processes to support your compliance with these requirements each calendar year. These Medicare Compliance Program requirements include, but are not limited to:

- Fraud, Waste and Abuse ("FWA") training, General Compliance training and Code of Conduct/Compliance policy distribution
- Exclusion list screenings



- Reporting FWA and compliance concerns to The Company
- Offshore operations & CMS reporting
- Model of Care Training
- Specific federal and state compliance obligations
- Monitoring and auditing of First Tier, Downstream and Related Entities

What may happen if you don't comply

If our FDRs fail to meet these Medicare Compliance Program requirements, it may lead to:

- Development of a corrective action plan
- Retraining
- Termination of your contract and relationship with The Company, Inc.

Our actions in response to a First Tier Entity's non-compliance will depend on the severity of the compliance issue. If a First Tier Entity identifies areas of non-compliance (e.g., refusal of an employee to complete the required FWA training), the First Tier Entity must take prompt action to fix the issue and prevent it from happening again.

Attestation requirements

You must to maintain evidence of your compliance with these Medicare Compliance Program requirements (e.g., employee training records, CMS certificate of FWA training completion, etc.) for no less than 10 years. Also, each year, an authorized representative from your organization must attest to your compliance with the Medicare Compliance Program requirements described in this guide. The authorized representative is an individual who has responsibility directly or indirectly for all:

- Employees
- Contracted personnel
- Providers/practitioners
- Vendors who provide healthcare and/or administrative services for Company's Medicare Plans

This could be your Compliance Officer, Chief Medical Officer, Practice Manager/ Administrator, Provider, an Executive Officer or similar related positions.

You may be asked to provide evidence of compliance

In addition to completing an attestation, Company and/or CMS may request that you provide evidence of your compliance with these Medicare Compliance Program requirements. This is for monitoring/auditing purposes.

We take these responsibilities very seriously. If you have questions or concerns about these Medicare Compliance Program requirements, just contact the Company Medicare Compliance Officer. What follows is a description of each Medicare Compliance Program requirement.



Fraud, Waste and Abuse (“FWA”) training, General Compliance training and Code of Conduct/Compliance policy distribution

FWA and general compliance training

As a First Tier Entity, you/your organization must provide FWA and general compliance training to all your employees and Downstream Entities assigned to provide administrative and/or healthcare services for our Medicare Plans. To comply with this requirement, you can use CMS’s Medicare Parts C & D Fraud, Waste and Abuse and General Compliance Training that is available out the CMS Medicare Learning Network (MLN) at <https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/providercompliance.html>.

Compliance training requirements

Regardless of the method used, the training must be completed:

- Within 90 days of initial hire or the effective date of contracting
- At least annually thereafter

Also, you must maintain evidence of training completion. Evidence of completion may be in the form of attestations, training logs, or other means determined by you to best represent fulfillment of your obligations. For convenience, there are certificates of completion included on the last slides of the *CMS Medicare Parts C & D Fraud, Waste, and Abuse Training and General Compliance Training*.

The only exception to this training requirement is if you/your organization is “deemed” to have met the FWA certification requirements through enrollment into Medicare Parts A or B of the Medicare program or through accreditation as a supplier of Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS). Those parties deemed to have met the FWA training through enrollment into the CMS Medicare Program don’t need to complete *Part 1: Medicare Parts C and D Fraud, Waste, and Abuse Training*. But, they’re still obligated to complete *Part 2: Medicare Parts C & D Compliance Training*.

You can find the training requirements and information regarding deemed status at:

- 42 C.F.R. § 422.503(b)(4)(vi)(C) for Medicare Advantage
- 42 C.F.R. § 423.504(b)(4)(vi)(C) for Part D
- Manual, Chapters 9 & 21 § 50.3

You must give your employees this Code of Ethical Business Conduct and Compliance for FDRs

Your organization must also provide either Company’s Code or your own comparable Code of Conduct/Compliance Policies to all employees and Downstream Entities who assigned to work on Company Medicare business for our Medicare Plans. You must distribute The Code:

- Within 90 days of hire or the effective date of contracting
- When there are updates to such Standards of Conduct
- Annually thereafter

Also, you must retain evidence of your distribution of the Code. You can find these the Code requirements in:



- 42 C.F.R. § 422.503(b)(4)(vi)(A) for Medicare Advantage
- 42 C.F.R. § 423.504(b)(4)(vi)(A) for Part D
- Manual, Chapter 9 § 50.1.1

Exclusion list screenings

Federal law prohibits Medicare, Medicaid and other federal healthcare programs from paying for items or services provided by a person or entity excluded from participation in these federal programs. Therefore, prior to hire and/or contract and monthly thereafter, each FDR must check the Office of Inspector General (OIG) and General Services Administration (GSA) “exclusion lists” to confirm that employees and Downstream Entities performing administrative and/or healthcare services for Company’s Medicare Plans aren’t excluded from participating in Federally-funded healthcare programs. You can use these websites to perform the required exclusion list screening:

- Office of Inspector General (OIG) List of Excluded Individuals and Entities at <http://exclusions.oig.hhs.gov>
- General Services Administration (GSA) System for Award Management (SAM) at <https://www.sam.gov/portal/SAM>

Also, FDRs must maintain evidence they checked these exclusion lists. You can use logs or other records to document that you’ve screened each employee and Downstream Entity in accordance with current laws, regulations and CMS requirements.

You must perform exclusion list screenings

You’re not alone. We’re also required to check these exclusion lists prior to the hiring or contracting of any new employee, temporary employee, volunteer, consultant, and Board of Director, and monthly thereafter. We cannot check these exclusion lists for your employees and Downstream Entities. So, to make sure we comply with this CMS requirement, you must confirm that your permanent and temporary employees and Downstream Entities that provide administrative and/or healthcare services for our Medicare Plans are not on either of these exclusion lists.

You must take action if an employee or Downstream Entity is on the list

If any of your employees or Downstream Entities are on one of these exclusion lists, you must immediately remove them from work directly or indirectly related to Company’s Medicare Plans and notify us right away.

These exclusion list requirements are noted in § 1862(e)(1)(B) of the Social Security Act, 42 C.F.R. §§ 422.503(b)(4)(vi)(F), 422.752(a)(8), 423.504(b)(4)(vi)(F), 423.752(a)(6), 1001.1901, and further described in the Manual, Chapters 9 & 21.



Reporting Violations to University of Maryland Health Advantage, Inc.

You have an obligation to report all suspected violations of the Code or any law or regulation, whether such violations involve your employees and Downstream Entities. There are a number of ways to report suspected or detected non-compliance or potential FWA. Don't worry – your reports are confidential.

You can make a report by taking any of the following actions:

- Call your Company contact.
- Call Company's Compliance Hotline at 410-779-9323.
- Send an email to Company's Compliance Department at Compliance@UMMSHealthplans.com

The Compliance Hotline is available 24 hours a day, seven days a week. Hotline calls are truly anonymous. Calls are not traced. There is no caller ID. The Hotline number is a voicemail number only. You will not speak to a person. If you do choose to make an anonymous report, be prepared to provide enough information about the situation to allow us to properly investigate it.

We provide all the information listed above on Company's "Know Your Compliance ABC's" poster that is provided at the end of The Code. You can share the poster with your employees and Downstream Entities. You can also keep it as a reference tool and use your own internal processes for reporting and collecting these issues. If you choose to your own processes, make sure you report it to Company.

You must adopt and enforce a zero-tolerance policy for retaliation or intimidation against anyone who reports suspected misconduct.

Medicare Compliance Officer

Dedicated to Company's Medicare Compliance Program is our Medicare Compliance Officer, who is based in Timonium, Maryland. Questions or concerns for the Medicare Compliance Officer can be sent to the following mailbox: Compliance@UMMSHealthplans.com

Non-Retaliation Policy

Company has a zero-tolerance policy for retaliation or retribution against any employee or FDR who, in good faith, reports suspected misconduct or Fraud, Waste, and Abuse (FWA). Intimidation or retaliation against any employee who cooperates in a compliance investigation is strictly prohibited and will lead to disciplinary action.

Company adheres to an anti-retaliation and anti-intimidation policy for good faith participation in the compliance program, including, but not limited to, reporting potential issues, investigating issues, conducting self-evaluations, audits and remedial actions, and reporting to appropriate officials. Intimidation or retaliation against any employee or FDR who cooperates in a compliance investigation is strictly prohibited. Company has adopted a zero-tolerance policy for retaliation or retribution against any employee or FDR who reports suspected FWA in good faith. The False Claims Act and other applicable regulations also protect employees and FDRs from retaliation for complaints.

Company is committed to prohibiting retaliation against those who report, oppose, or participate in an investigation of alleged wrongdoing in the workplace. By way of example only, participating in an investigation of alleged wrongdoing in the workplace, includes, but is not limited to:



- Filing a complaint with a federal or state enforcement or administrative agency;
- Participating in or cooperating with a federal or state enforcement agency that is conducting an investigation of Company regarding alleged unlawful activity;
- Testifying as a party, witness, or accused regarding alleged unlawful activity;
- Associating with another employee who is engaged in any of these activities;
- Making or filing a complaint with Company regarding alleged unlawful activity;
- Providing informal notice to Company regarding alleged unlawful activity.

Company strictly prohibits any adverse action/retaliation against an employee for participating in an investigation of any alleged wrongdoing in the workplace.

Your Obligation to Cooperate in Investigations

Company promptly investigates all reported or suspected violations of the Code and maintains confidentiality to the extent possible.

All FDRs must cooperate fully and honestly in any Company investigation or inquiry by Company management, outside auditors, or government officials. You must provide all applicable documents when responding to an investigation or audit and must not destroy or alter any records.

Keep in mind that Company does not tolerate discrimination of or retaliation against anyone who in good faith makes a report or participates in an investigation.

Offshore operations & CMS reporting

To help make sure we comply with applicable federal and state laws, rules and regulations, you're prohibited from using any individual or entity (Offshore Entity) to perform services for Company's Medicare Plans if the individual or entity is physically located outside of one of the fifty (50) United States or one of the United States Territories (i.e., American Samoa, Guam, Northern Marianas, Puerto Rico, and Virgin Islands). The only exception to this is if an authorized Company representative agrees in advance and in writing to the use of such Offshore Entity.

Notify us immediately if you plan to use an Offshore Entity

If you perform services offshore or use an Offshore Entity to perform services involving the receipt, processing, transferring, handling, storing, or accessing of Medicare Member protected health information (PHI) and we approve the arrangement, we must submit an attestation to CMS. One example provided by CMS of offshore services that trigger this attestation requirement is "offshore subcontractors that receive radiological images for reading, because beneficiary personal health information (PHI) is included with the radiological image and the diagnosis is transmitted back to the U.S." Therefore, you must immediately notify Company Medicare Compliance Officer if you plan to use an Offshore Entity.

Model of Care Training

Over the years CMS has become increasingly focused on the care management processes for its beneficiaries who are enrolled in Special Needs Plans (SNP). In 2008, the Medicare Improvements for Patients and Providers Act (MIPPA) mandated that all SNPs design and implement evidence-based Models of Care (MOC) to support the unique health care needs of special needs individuals and the most vulnerable beneficiaries they serve. MOCs help ensure that the unique needs of each enrolled beneficiary are identified and addressed. Furthermore, MOCs provide the needed infrastructure to promote quality care management and care coordination processes.



In 2010, the Patient Protection and Affordable Care Act (PPACA) reinforced the importance of the MOC as a fundamental component of the SNP quality improvement framework by requiring the National Committee for Quality Assurance (NCQA) to execute the review and approval of SNPs' MOC based on standards and scoring criteria established by CMS. One of the scoring elements focuses on Model of Care Training for network providers.

As a Medicare Advantage Organization offering a Dual-Special Needs Plan, we must ensure that all network providers and FDRs who provide and/or arrange for healthcare services to our members complete Company's Model of Care Training at the time of contracting and annually thereafter. Company must maintain documented evidence that it makes available and offers training on the Model of Care to its network providers and other FDRs. The Model of Care Training is provided at <http://www.umhatraining.com> and is also available on the health plan's Provider Portal at www.UMMedicareAdvantage.org.

Specific federal and state compliance obligations

Based upon the services that you/your organization performs for Company's Medicare plans, you may be subject to other federal and state laws, rules and regulations that we didn't describe in the Code. If you have questions about the Medicare compliance requirements for the services that you/your organization perform, consult Company's Medicare Compliance Officer.

Monitoring and auditing of First Tier and Downstream Entities

CMS requires that we develop a strategy to monitor and audit our FDRs. This helps ensure compliance with all applicable laws and regulations and that our First Tier entities monitor the compliance of their Downstream Entities. Therefore, if you choose to subcontract with other individuals/parties to provide administrative and/or healthcare services for Company's Medicare Plans, you must make sure that these Downstream Entities abide by all laws and regulations that apply to you as a First Tier Entity. This includes the Medicare Compliance Program requirements described in the Code.

Also, you/your organization must conduct sufficient oversight to test and ensure that your employees and Downstream Entities are compliant with applicable laws, retain evidence of completion, conduct root cause analysis and implement corrective action plans or take disciplinary actions, as necessary, to prevent recurrence of non-compliance with applicable laws.

Expect routine monitoring and audits

We routinely monitor and periodically audit First Tier Entities. This helps us ensure compliant administration of our contracts with CMS to offer Medicare Plans, as well as applicable laws and regulations. Each First Tier Entity must cooperate and participate in these monitoring and auditing activities. If a First Tier Entity performs its own audits, we may request the audit results affecting Company's Medicare business. Also, we expect First Tier Entities to routinely monitor and periodically audit their Downstream Entities.

If we determine that an FDR doesn't comply with any of the requirements in this guide, we will require the FDR to develop and submit a Corrective Action Plan (CAP). We can help the FDR address the identified compliance issues.

These Monitoring and Auditing requirements are noted in 42 C.F.R. §422.503(b)(4) (vi)(F) for Medicare Advantage and 42 C.F.R. §423.504(b) (4)(vi)(F) for Part D, and further described in the Manual, Chapters



9 & 21.

University of Maryland Health Advantage’s Workplace Standards and Practices

Company is committed to providing a safe, healthful, and secure work environment.

Workplace Violence

Company does not tolerate any form of violence, threats, harassment, intimidation or other disruptive behavior in the workplace. This includes verbal or written threats of violence.

Weapons

Weapons of any sort are prohibited on Company-owned or leased premises and while conducting Company business. This applies even if you have a permit or license to carry a weapon.

Smoke-Free Workplace

Smoking is prohibited throughout Company’s location. This includes the building and building entrances.

Drug-Free Workplace

Company complies with the Drug-free Workplace Act of 1988. Company expects its workforce to report to work free from the influence of illegal drugs and alcohol. Company strictly prohibits the use, abuse, sale, purchase, possession, manufacture, or distribution of any intoxicating or illicit substances in Company workplace, on Company owned or leased premises, or while representing Company at any time.

Health, Safety, and Environment

You are required to obey safety rules and regulations when on-site and to notify your Company business contact of any circumstances that may be potentially harmful to the health and safety of any individual on Company premises or to the environment.

When on-site, you and your employees and contractors must work in conformance with all applicable safety rules, laws, standards and procedures, including Occupational Safety and Health Administration (“OSHA”) rules and regulations and any additional requirements of Company.

Solicitation, Distribution of Materials and Bulletin Boards

Company bulletin boards are limited to Company sponsored or generated material and Company business-related material. Postings of any communications in common areas, such as near elevators or in hallways, are prohibited.

Solicitation or distribution of non-job related material must be approved by Company management and is restricted to break times.



Communications and Distribution

Company's Medicare Compliance Department maintains effective and appropriate lines of communication with all key stakeholders of the organization, including:

- All levels of management, the President & CEO, and Board of Directors
- The Medicare Compliance Committee
- Company employees at all levels
- Contracted partners, especially providers and marketing representatives
- FDRs
- Regulatory authorities
- As may become necessary, law enforcement agencies

The Medicare Compliance Department will use these lines of communication to effectively communicate information about the Medicare Compliance Officer (e.g., the Medicare Compliance Officer's name, office location, and contact information), as well as information about laws, regulations, and guidance for the health plan and its FDRs, such as statutory, regulatory, and sub-regulatory changes (e.g., HPMS memos) and changes to policies and procedures and the Code.

These lines of communication will be accessible to all and allow for anonymous and confidential good faith reporting of potential compliance issues as they are identified. Confidentiality will be maintained to the greatest extent possible.

It is mandatory for employees, members of the governing body, and FDRs to report compliance concerns and actual or suspected FWA to Company's Medicare Compliance Department. The Medicare Compliance Department communicates this mandatory reporting requirement through training, compliance presentations, and disciplinary actions.

The Medicare Compliance Department also maintains a system to receive, record, respond to and track compliance issues, reports of suspected or detected non-compliance, or fraud, waste, and abuse from employees, members of the Board, enrollees and FDRs. The Medicare Compliance Officer is the owner of these records and documents.

It is our expectation that all FDRs will share any communications sent by the Medicare Compliance Officer to its employees who assigned to work on Company's Medicare business for our Medicare Plans.

Communications and Public Affairs

While we respect our FDRs' right to discuss their products or services with the media, FDRs are not authorized to speak about or on behalf of Company without our prior approval.

In the event that you receive an inquiry regarding any facet of Company's business, please refer the inquiring individual to our Public Affairs department. Whenever possible, please contact our Public Affairs department to let us know of the inquiry.



FDR Relationships with Company Employees

Offers to Company employees from FDRs, vendors or suppliers have the potential to be perceived as bribes, kickbacks, or unfair sales practices and could violate Company policies and laws.

Accordingly, you should be aware that Company employee are not allowed to participate in the following activities:

- Receiving cash directly or indirectly from an external source without any services of comparable value,
- Receiving products or services for free or at less than fair market value from any outside source, including but not limited to:
 - o Materials and/or products to be distributed internally or externally
 - o Offers to provide research and data results at no cost to Company
 - o Offers to conduct mailings on Company's behalf at no cost to Company
 - o Offers to perform free seminars for associates or customers
 - o Participation in joint activities, such as health fairs or other marketing activities
 - o Waiver of seminar fees with the exception noted below*
 - o Offers to participate, without cost to Company, in industry-related meetings which involve travel, meals, or entertainment
 - o Receiving anything with more than a nominal value from an external source, for which no payment or payment of less than fair market value by Company is involved.
 - o Company employees may not accept offers from FDRs, a vendor or supplier to pay the associate's travel and lodging expenses to attend a conference sponsored by the vendor or supplier.

* If the associate is speaking at the conference, meeting, or seminar, the registration fee typically can be waived if the fee is also being waived for other speakers.

Confidential and Proprietary Information

You are responsible for safeguarding Company's confidential and proprietary information both during and after the term of a contract or engagement as an FDR. You are responsible for ensuring that such information is used only for valid business purposes and not to provide personal gain for yourself or others.

When using social media, you may not discuss or disclose confidential or proprietary and/or financial information about Company, associates, members, providers, partners, clients, vendors or suppliers.

University of Maryland Health Advantage, Inc. Electronic Assets

Email, Internet, Intranet, telephone, voice mail system, instant messaging, fax equipment, and other electronic means supplied by Company are Company assets to be used for legitimate business purposes or for purposes authorized by management. You must follow the policies, procedures, standards, and guidelines that relate to Company's electronic assets at all times and at all work sites. This includes while tele-working from non- Company sites.

You do not have an expectation of privacy when using Company's electronic communication systems. Company has the right to review, copy, audit, investigate, intercept, access, and disclose any use of the



computer, e-mail, instant messaging, telephone, and Internet systems, including all messages created, received, or sent for any purpose.

The contents of electronic storage (e.g. e-mail, instant messaging) may be disclosed within Company and to government agencies without your knowledge or permission. Access by management is permitted without your consent and without giving prior notice.

When your engagement or relationship with Company ends, or upon Company's request, you must return any and all Company assets in your possession.

University of Maryland Health Advantage, Inc. Records, Record Retention and Destruction

You must ensure that facts are never misstated or material information omitted to Company, and that all records, disclosures and communications to Company are full, fair, accurate, timely and understandable.

Destroying or disposing of Company records is not at your individual discretion. Destruction, alteration, or falsification of records to avoid disclosure in a legal proceeding, government investigation or audit may constitute a criminal offense.

Passwords and Access Codes

You may not share any Company system passwords or access codes with anyone. Failure to comply will result in the removal of your access and termination of your Agreement with Company.

Security Requirements

You must adhere to Company security requirements, practices, and procedures. Standard facility access policies and procedures have been established to provide specific guidelines for FDR access to Company facilities. FDRs must promptly report any activities that may compromise the security and the confidentiality of Company's data to their Company business contact or the Medicare Compliance Officer.

Compliance with Company security requirements includes, but is not limited to the following:

Connectivity: Non-Company equipment may not be directly connected to Company infrastructure without prior approval. At Company locations, access for computers supplied by FDRs may be available via segregated wireless connectivity.

User ID and Accounts: On an as-needed basis, Company provides a login ID and password for FDR personnel, subject to all applicable Company policies and procedures regarding usage and password strength. IDs and passwords are unique to each individual and must not be shared with others. All accounts will be disabled promptly upon the completion of the contract or engagement. IDs are configured to expire on a particular date depending on the business contract or assignment. Any extension request must be submitted in writing and approved by the Company Business Owner.

Company Confidential Information Including Protected Health Information ("PHI") and Personally Identifiable Information ("PII"): Any Company Confidential Information acquired or accessed during the course of a contract or engagement must be used and safeguarded in accordance with the strictest application of the minimum necessary standard (the minimum amount necessary to accomplish the



intended purpose of the use or disclosure of or request for the Confidential Information) as required by regulation and Company policy.

Company Assets: The use of Company assets, including desktop, laptop, e-mail, etc. are for business use only.

E-Mail: Appropriate Company processes must be used to protect any e-mail containing Company Confidential Information. Always assume that the content of outgoing e-mail is Confidential Information and use the secure e-mail procedures that are available on Company intranet. You may be personally liable for failure to protect Company Confidential Information.

Laptops: Company requires encryption of all laptops in order to render the information unusable and unreadable in the event of an inadvertent loss or disclosure. Company issued laptops, when unattended, must be secured with the provided cable locking device. Unsecured, unattended laptops are subject to confiscation and removal by Solutions.

Removable Media: The use of removable media is discouraged. Company requires encryption of all removable media in order to render the information unusable and unreadable in the event of inadvertent loss or disclosure.

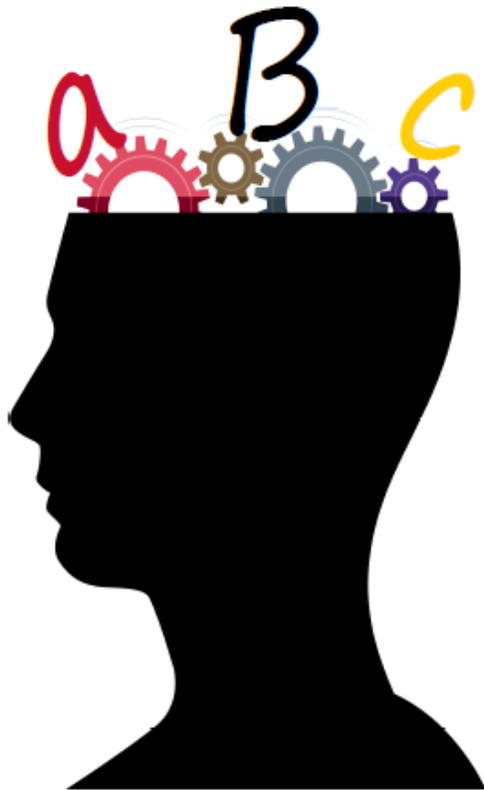
Risk Assessment: Company may ask for verification or qualification of the security process of any FDR in order to safeguard both Company Confidential Information and assets and any third party software and to better understand the potential risks associated with the contracted services.

Questions/Concerns

For compliance questions or concerns, you can email the Company Compliance mailbox:

Compliance@ummshealthplans.com.

Think Different.
Know your Compliance ABC's.



*A*ctively listen. *B*e proactive. *C*ommunicate effectively.

Report suspected Fraud, Waste, and Abuse, Compliance issues, or misconduct without intimidation or fear of retaliation.

**Compliance Anonymous Hotline:
410.779.9323**

**Email:
Compliance@UMMSHealthplans.com**

**Compliance Officer:
Mary-Paul Snapp-Borleis**



UNIVERSITY *of* MARYLAND
HEALTH **ADVANTAGE**