Quality health plans & benefits
Healthier living
Financial well-being
Intelligent solutions

aetna®

# FDR Compliance Newsletter

October 2018 – Issue 19

## Removal of fraud, waste and abuse (FWA) training requirement

The Centers for Medicare & Medicaid Services ("CMS") enacted a Final Rule effective June 15, 2018. This rule will remove the requirement for FDRs to complete CMS-issued general compliance and FWA training beginning in 2019.

Aetna will continue to conduct routine monitoring, auditing and oversight of our FDRs. This will include reviews of the Medicare compliance program requirements.

Starting in 2019, we will assess the following elements:

- Standards of conduct and/or compliance policies
- U.S. Department of Health & Human Services Office of Inspector General (OIG) and General Services Administration's System for Award Management (SAM) exclusion screening
- Reporting mechanisms
- Downstream entity oversight
- Operational oversight

Please review the most updated FDR Guide, and ensure you have internal processes in place to support your compliance with these requirements.

## In this issue



## Quick links

- **Archived newsletters**
- **Aetna's FDR Guide** (updated 3/2018)
- **Medicare Managed Care Manual**
- **Medicare Prescription Drug Benefit Manual**
- **Aetna's Code of Conduct** (updated 12/2017)
- **CMS's General Compliance Training**
- **CMS's FWA Training**
- **Exclusion lists:**
  - **OIG's List of Excluded Individuals and Entities (LEIE)**
  - **GSA's System for Award Management (SAM)**

*Aetna maintains a comprehensive Medicare Compliance Program. It includes communication with Aetna Medicare FDRs. Dedicated to Aetna's Medicare Compliance Program is John Wells, Medicare Compliance Officer. He's based in Maryland. You can send questions or concerns to* ***MedicareFDR@aetna.com*****.**

## Restoration of the MA OEP, change to the Dual/LIS SEP and other enrollment updates

In April 2018, CMS issued final regulatory guidance regarding the restored Medicare Advantage Open Enrollment Period ("MA OEP"), and modified and updated several Special Enrollment Periods (SEPs). Since April, CMS has released marketing and enrollment guidance clarifying how to handle such periods in the marketplace. The following provides highlights of the MA OEP and the SEP for Dual and Low Income Subsidy (LIS) eligibles.

**Medicare Advantage Open Enrollment Period ("MA OEP" or "OEP"):**

This period will allow all MA enrollees to make a change January 1 through the end of March. Those beneficiaries who are newly eligible for MA will have that OEP and it will occur the first three months in which they have both Part A and Part B. During the OEP, individuals will be able to enroll in another MA plan, with or without prescription drugs. Or they could choose to return to Original Medicare, picking up a stand-alone part D plan if they would like. The OEP does not, however, provide those in Original Medicare the option to join an MA plan. This OEP is limited only to those enrolled in a Medicare Advantage plan.

CMS has put strict marketing restrictions in place for the MA OEP. Please make sure to review the requirements to know what you can and can't do during this period. You can find detail on the MA OEP marketing restrictions in the recently released CMS Medicare Communications and Marketing Guidelines.

**SEP for Dual and other LIS individuals**

The key change to this SEP is the timing. This SEP now allows a quarterly change from January through September. Previously, duals (those eligible for both Medicare and Medicaid) and those with LIS had an "ongoing" SEP, permitting the ability to change plans every month. Between October and December, dual and LIS individuals will have the Annual Enrollment Period to make changes. This SEP is not available to any individual that CMS identifies as an "at risk" or "potentially at risk" for misuse or abuse of frequently abused prescription drugs.

More detail for all enrollment periods updates, including the SEP for those impacted by disasters, can be found in the updated CMS Medicare Advantage and Part D enrollment guidance documents.

It is imperative all plans, including agents who sell such plans, take appropriate steps to validate a beneficiary's status before submitting an enrollment. This helps ensure a smooth and positive experience for all prospective members.

## Common FDR CPE audit review findings

Aetna conducts routine monitoring, auditing and oversight of our FDRs against the Medicare Compliance Program Effectiveness (CPE) requirements.

We commonly identify that our first tiers lack sufficient oversight of their downstream entities, including prior to contracting and monthly Office of Inspector General List of Excluded Individuals and Entites and General Service Aadmininstration System for Award Management screening.

To help you with overseeing your downstream entities, Aetna's FDR Guide includes a toolbox of resources for you to utilize.

This quarter we would like to highlight the use of a self -assessment tool that can be modified and used to assess the compliance of your downstream entities.

### What is an FDR

**FDR = First tier, downstream and related entities**

A **first tier** entity is any party that enters into a written arrangement with our organization to provide administrative or health care services for our Medicare business.

A **downstream** entity is any party that enters into a written arrangement with persons or entities below the level of the first tier's arrangement with our organization. These arrangements continue down to the level of the ultimate provider of both health and administrative services.

A **related** entity is an entity that is linked to our organization by common ownership or control and provides functions to support our Medicare business.

## The three T's

I'd like to share a story with you. The facts of the story are accurate but I changed the names of those involved. It's a story of the pursuit of efficiency and effectiveness by a relatively small organization absolutely committed to the long term health and success of their clients. I'll introduce you to Tony, a very successful insurance broker that offers his clients health care insurance (Medicare) and other insurance products from multiple carriers. Tony has been in business for decades and he enjoys a comfortable lifestyle as a result of the many clients that rely on him to address their well-being.

Tony has an office manager named Tina, who has worked for Tony for many years.She is bright, talented and committed to the success of Tony's firm. Tina loves to read on-line business publications from her tablet when she commutes to and from work on the bus each day. Tina is fascinated with business information and she is particularly interested in technology companies, along with the explosive growth of these industry leaders and impact on the consumer.

One day during Tony's staff meeting he asked for any ideas or feedback from his staff. Tina recognized the opportunity and immediately suggested that she lead a project. She planned to back up all of the office workstations and

the file servers using a cloud service that has a significantly lower cost, while also backing up files at another location for better business resiliency. Tony loved the idea and had confidence in Tina, so he asked her to lead the effort and report back to the team. Tina was thrilled with the opportunity and immediately started the project. She selected the industry leader in infrastructure services (Amazon Web Services) and selected the S3 Bucket service option to meet the business needs.

The implementation went smoothly and Tony praised Tina at subsequent staff meetings. There was little to no friction for the other agents and administrative staff in the implementation. Tina was promoted to office manager and continued to learn more about emerging technology for office workers while improving existing business processes.

Over a year following the implementation of this capability an independent security researcher, named Chris, developed a methodology to search for AWS S3 buckets that were not configured with authentication or encryption capability. Chris published the results on a website for a vulnerability management vendor. Several clients called the office concerned about the article and related security breach and Tina immediately contacted AWS and changed the configuration to include authentication and encryption of the data in the bucket. Tina met with Tony and their compliance officer to make them aware of the breach and to plan their approach to address the client concerns. The compliance officer began preparation of the regulatory notification since the data exposed included several hundred thousand health insurance applications from multiple carriers with client information (PII and PHI). The compliance officer suggested that Tina hire a security firm to do a forensic review to determine the scope of the exposure for reporting purposes.

Tina felt badly that she let Tony and their clients down. She had decided not to add authentication to the S3 bucket when she set it up since she knew Tony forgets his passwords regularly. And the url for the S3 bucket was so lengthy that she figured it was safe enough. She didn't encrypt the data since it cost more money for that service. After the forensic analysis was completed she learned that there was no application logging turned on. So there was no way to determine if anyone besides the security researcher had access to the data. The HIPAA violation fines would be based on all of the data included in the breach scope. The costs of the forensic review and the potential HIPAA violation fines were a significant impact to Tony's brokerage business. There were many clients that took their business elsewhere. Tina was dismayed that something so promising turned out to have such negative consequences for her and for the business.

Tina immersed herself into cyber security practices for protecting client information. She got access to information from the insurance carriers on specific procedures for configuring cloud hosting services to set up:

1. Multi-factor authentication
2. Data encryption
3. Event logging
4. Incident response support

She also learned that agents using laptops need to have full disk encryption configured to protect against the potential for a breach if a

laptop is lost or stolen. She advised agents to use this url to check to determine if their laptop has encryption:

https://www.encryptmylaptop.com

Tina prepared a communications program for all agents and employees on cyber tips to keep client data safe, and she led webinars to educate them on leading data protection practices. She enrolled in a master's program in cyber security and found something else that she was passionate about besides business news. Tony was proud of what Tina learned and over time he experienced substantial growth in his business based on clients that appreciated the cyber security program in place to protect their sensitive data.

The story of the three T's could have been Tony, Tina and Trouble. But based on Tina's contributions to improvements in data security it is Tony, Tina and Thanks from all of the clients!

**Report to Aetna actual or potential fraud, waste and abuse OR non-compliance:**

FDRs can have their own internal processes in place for reporting, however, instances which impact Aetna's Medicare business should be reported back to us by using one of the methods below:

By phone:
**1-888-891-8910**
(7 days a week, 24 hours a day)

Over the internet:
**https://aetna.alertline.com**

By mail:
**Corporate Compliance**
**P.O. Box 370205**
**West Hartford, CT 06137-0205**