

Congressional Testimony of Charlene Frizzera  
President and CEO, CF Health Advisors  
Committee on Ways and Means Subcommittee on Oversight  
March 24, 2014

I want to thank Congressman Roskam and the other committee members for inviting me to testify today about predictive analytics for detecting Medicare fraud. My name is Charlene Frizzera and I had the pleasure to work at CMS for over 30 years. During my time at CMS I worked in the Medicare and Medicaid programs and on broader health reform initiatives with the passage of the ACA. I served as the Regional Administrator in the Philadelphia Regional Office under Nancy Ann DeParle, the Deputy Director of the Medicaid and CHIP programs under Tom Scully the Chief Operating Officer under Mark McClellan and was the Acting Administrator from January, 2009 until Marilyn Tavenner and Don Berwick came to CMS.

The people who work at CMS believe in the responsibility of taking care of beneficiaries and work hard to fulfill that goal. However, they are often faced with goals that change significantly over time and rules and procedures that can often prevent them from applying more rapid or innovative solutions to their goals. The one thing that we have learned is that fraud is hard to detect and stop. Preventing fraud is so difficult because the schemes and participants are constantly changing, adapting, and evolving to elude enforcement actions.

As fraud evolves, we must realize that our systems to detect and prevent fraud must change as well. I believe that the two main areas that should receive greater attention from lawmakers are the rules and processes that govern what the agencies can do to detect and prevent fraud and the technologies available today that can better aide us in better detection and prevention.

The Fraud Prevention System (FPS)

The goal of the FPS is to identify and prevent fraud, waste, and abuse in the Medicare Fee-For-Service program. The system identifies questionable billing patterns and aberrancies and provides information through an alert system report to the Zone Program Integrity (ZPIC) contractors. The ZPICs are then tasked with the follow up investigation of the provider.

The success of FPS is measured by the amount and speed with which it helps CMS and law enforcement detect fraud and how much potential fraud it uncovers. This is a different metric than simply looking at the amount that CMS actually recovers causing some difficulty in evaluating the performance of the program. The CMS June 2014 Report to Congress on the Fraud Prevention System Second Year Implementation indicated that FPS has saved \$210.7M in its first two years of implementation and \$54.2M in adjusted savings, which is money that is already returned or likely to be returned. CMS indicated the return is \$5 to every \$1 invested, however, the GAO, in their June 2014 report to Congress on the FPS, indicated the return was \$1.34 for every \$1.00 invested. This difference seems to be the inclusion by CMS of savings that either

cannot be substantiated or were not attributable to FPS. The usage of the adjusted savings metric by CMS makes it very difficult to separate the results of the FPS from the results of the ZPICs more generally.

In order to determine savings, there should be a clear accountability of the savings directly attributable to FPS. You can't improve the system if you are not able to justify the real results of the impact of the FPS. Further, it is difficult to assess the real returns of the FPS when we have no control group or other method to compare the FPS against. Under the current system ZPICs get information from many sources, one of which is the FPS. Contractors are held to performance standards and want to stop or prevent as much fraud as possible. In some cases, leads generated by other sources (i.e. beneficiary complaints) are more reliable than those of FPS. In these cases, the ZPIC does and should go with the lead that is the most reliable. The overlap of effort and lack of accountability attributable to the savings, makes an evaluation of the effectiveness of FPS difficult and makes it even more difficult to measure the FPS against what the ZPICs could have accomplished on their own.

#### Better Approaches to Using Technology

The impact of FPS to date has been to basically get data more quickly to contractors, but it uses the data as it exists today built off of a silo driven FFS database that is not multi-variant and is limited in its design. We currently have access to greater amounts of data and the technology to share that data in a much greater capacity than is utilized by the FPS.

The legislation provides broader authority for CMS to engage the industry than it had taken advantage of. The current FPS develops software to do predictive analytics. However, the definition of predictive analytics is limited to identifying providers that have similar circumstances of known bad actors and then linking them through addresses or phone numbers. This system makes sense, but is fundamentally limited for several reasons.

First, it is set up to detect fraud that is based on historical patterns. This approach is productive, but limits our thinking to exclude other ways that we could identify fraudulent behavior before a historical pattern has been established. Therefore, we are only able to predict fraud that copies a familiar pattern and are not able to identify new patterns of fraudulent behavior as quickly. By limiting our data set to these variables, we miss associations that could be identified with broader data sets integrated into the system. For example, using Tax Identification Numbers from the IRS would allow us to create links between entities that may be different providers in different states with normal spending patterns, but are linked to a single individual who is perpetrating the fraud across multiple provider entities so as to avoid detection. By limiting our data sources and only using historical patterns, we may very well be allowing more effective fraud schemes over time since we are effectively handing over our playbook to those looking to commit fraud.

Second, our ability to create informational associations should be inter-agency and use a

dynamic, more open network of information rather than a closed, fully proprietary system. Under the current contracting rules, the government owns the data and the intellectual property driving the system. Both of these discourage innovation. I appreciate the concerns about providing data more broadly and the concern about not owning the intellectual property. However, there exists a faulty underlying assumption in this approach that CMS has the best data and fraud detection tools available. We currently do not fully know if there are commercial insurance plans, other private third-party program integrity contractors, or even Medicaid programs that have better systems or tools to detect fraud than our current systems. A reasonable solution would be to allow the use of information from 'authorized sources', those sources that CMS already entrusts with other pieces of intellectual property, such as States, commercial plans, and contractors in other areas of program integrity outside the Medicare FFS system, to create a more robust database that will allow for connections that are potentially being overlooked due to a lack of unified database of information.

Our current closed system does not allow for this type of analysis. For example, on the second page of the Executive Summary on the 2014 Report to Congress, CMS highlights in a box on the top of the page that they prevented \$700,000 of inappropriate billing. This was accomplished by the FPS identifying inappropriate billing, having the contractor conduct a site visit, interviewing beneficiaries, and reviewing medical records. This is a good accomplishment that clearly was the result of a lot of hard work and coordinated effort. The real question though is whether this could have been accomplished with a more effective use of non-traditional data. Was this provider already excluded from commercial or Medicaid plans for fraud? Now, in this specific example, that might not be the case, but since there is no inter-agency coordination currently we don't know the answer. A simple matching of excluded providers from Medicaid agencies and Medicare Advantage plans may have yielded the same result with greater speed and less resources.

The technology available today in the private sector has the ability to rapidly integrate a greater number of data sets and make more effective associations between this data than is currently being used by CMS. The ability to use these more advanced systems and processes is limited by the rules and processes under which CMS is required to operate.

#### My Experience with the Miami Regional Office

To highlight these issues, I wanted to leave you with a personal experience that I had while I was the Acting Administrator. I travelled to the Miami Regional Office for a site visit to better understand what the current issues with the program integrity process were at that time. The staff in Miami first showed me a list of the top ten physicians with the highest billing in one county. The top three were off the charts. This information is similar to what the FPS currently provides to the ZPICs today. When I asked them what they do with this list, they told me they send it to the OIG for a decision on whether they will "take the case". In the meantime, CMS continues to pay the claims. Once they get an answer from OIG which could take months, many are no longer in practice so they cannot be found and the money is never recovered. As simple change in the rules to expedite this process or freeze payments pending the OIG investigation could have saved months of fraudulent claims from being paid. The FPS does have systems in place that

certainly improve on this process, but the delayed decision-making still hampers our system today.

Later, on the same visit, we then got in the car and drove to check out the physical locations of some of the providers. One of the sites was a storage space. When I said we should stop paying claims, they told me we couldn't until the NCS, the Medicare contractor that handled provider enrollment, visited the location and verified what we had just seen. Today, anyone with access to the internet can use Google Maps to almost instantly call up a picture of the street view of any address in the country. Now, this will of course not always provide the immediate answer in all potential fraud cases, but using technology to increase the speed and efficiency of the process of fraud detection is clearly a first step. Our understanding of the uses of technology should not be limited to simply the claims data and better algorithm to predict abhorrent spending. There can potentially be greater gains from thinking about how we can apply outside technologies to streamline and ease the human decision making factors that drive prevention.

My experience in Miami left me frustrated with the current rules and procedures that limited the ability, even as the Acting Administrator, to put a swift end to clear cases of fraud in the Medicare program. Since leaving the government, I have had the opportunity in the private sector to witness the technological capabilities available today and to better understand new approaches to program integrity efforts that could further strengthen the efforts of CMS if implemented.

### Conclusion

Doing something the same way and expecting a different answer doesn't work. Keeping the rules and process the same will not allow any new ideas and/or innovation to take place. A combination of new thinking and the use and existence of new technology are important considerations in continuing to improve the government's effort to fight fraud, waste and abuse.

The ability of CMS to fight and prevent fraud in the Medicare system is limited to the information it has available and the rules that govern the procedures to investigate and stop fraud. Those looking to commit fraudulent schemes do not face the same limitations. The majority of program integrity initiatives to date have simply been to add new systems and processes on top of an existing infrastructure that has not kept pace with technological innovation and the programmatic changes that have occurred.

Lastly, fraud is not limited to the Medicare FFS system. Commercial plans, Medicaid programs, the Treasury Department, and other commercial entities are currently trying to address these same issues with fraudulent schemes designed to take advantage of lapses in program integrity in the health care system. Today, we have the technological capabilities to integrate these efforts and communicate information and best practices with speed and efficiency. To truly stay one step ahead of fraud, we need to design a system of processes and procedures that integrate the wealth of information and data available to us today to analyze and detect fraud. This should include not just better technology, but a systemic and holistic overhaul and redesign of the people and processes

that we use for program integrity efforts. Those looking to commit fraud face no legal or procedural barriers to develop and operate fraudulent schemes. We should give those tasked with identifying and preventing these schemes the best information, procedural architecture, and flexibility to ensure the continued integrity of government healthcare programs and payments.