April 24, 2012

MEDICARE

Important Steps Have Been Taken, but More Could Be Done to Deter Fraud

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-671T, a testimony before the Committee on Finance, U.S. Senate

Why GAO Did This Study

GAO has designated Medicare as a high-risk program, in part because its complexity makes it particularly vulnerable to fraud. Fraud involves an intentional act or representation to deceive with the knowledge that the action or representation could result in gain. The deceptive nature of fraud makes its extent in the Medicare program difficult to measure in a reliable way, but it is clear that fraud contributes to Medicare's fiscal problems. Reducing fraud could help rein in the escalating costs of the program.

This statement focuses on the progress made and steps that remain to be taken by CMS to implement recent legislation and GAO's past recommendations to prevent or reduce fraud in Medicare. It is based on relevant GAO products issued from April 2004 through April 2012 using a variety of methodologies, such as analyses of Medicare claims, review of relevant policies and procedures, and interviews with officials. In April 2012, GAO also received updated information from CMS on agency actions.

View GAO-12-671T. For more information, contact Kathleen King at (202) 512-7114 or kingk@gao.gov.

What GAO Found

The Centers for Medicare & Medicaid Services (CMS)—the agency that administers Medicare—has made progress in implementing several key strategies GAO identified in prior work as helpful in protecting Medicare from fraud; however, some actions that could help combat fraud remain incomplete.

Provider Enrollment: GAO's previous work found persistent weaknesses in Medicare's enrollment standards and procedures that increased the risk of enrolling entities intent on defrauding the program. CMS has strengthened provider enrollment—for example, in February 2011, CMS designated three levels of risk—high, moderate, and limited—with different screening procedures for categories of providers at each level. However, CMS has not completed other actions, including implementation of some relevant provisions of the Patient Protection and Affordable Care Act (PPACA). Specifically, CMS has not (1) determined which providers will be required to post surety bonds to help ensure that payments made for fraudulent billing can be recovered, (2) contracted for fingerprint-based criminal background checks, (3) issued a final regulation to require additional provider disclosures of information, and (4) established core elements for provider compliance programs.

Pre- and Post-payment Claims Review: GAO had previously found that increased efforts to review claims on a prepayment basis can prevent payments from being made for potentially fraudulent claims, while improving systems used to review claims on a post-payment basis could better identify patterns of potentially fraudulent billing for further investigation. CMS has controls in Medicare's claims processing systems to determine if claims should be paid, denied, or reviewed further by comparing information on claims with information on providers and Medicare coverage and requirements. These controls require timely and accurate information about providers that GAO has previously recommended that CMS strengthen. GAO is currently examining CMS's use of prepayment edits to implement coverage and payment policies and CMS's new Fraud Prevention System, which uses analytic methods to examine claims before payment. CMS could better use post-payment claims review to identify patterns of fraud by incorporating prior GAO recommendations to develop plans and timelines for fully implementing and expanding two information technology systems it developed. These systems are a central storehouse of Medicare and other data and a Web portal to the storehouse with tools for analysis.

Robust Process to Address Identified Vulnerabilities: Having mechanisms in place to resolve vulnerabilities that lead to erroneous payments is critical to effective program management and could help address fraud. Such vulnerabilities are service- or system-specific weaknesses that can lead to payment errors—for example, providers receiving multiple payments as a result of incorrect coding. GAO has previously identified weaknesses in this process, which resulted in vulnerabilities being left unaddressed. GAO is evaluating the current status of the process for assessing and developing corrective actions to address vulnerabilities.