Testimony Before the United States House of Representatives

Committee on Oversight and Government Reform:

Subcommittee on Government Operations

Subcommittee on Intergovernmental Affairs

Improper Payments in State-Administered Programs: Medicaid

Testimony of:

Megan H. Tinker
Senior Advisor for Legal Review
Office of Counsel to the Inspector General
Office of Inspector General
Department of Health and Human Services

April 12, 2018
10:00 a.m.
2154 Rayburn House Office Building

Testimony of:
Megan H. Tinker
Senior Advisor for Legal Review
Office of Inspector General, U.S. Department of Health and Human Services

Good morning, Chairmen Meadows and Palmer, Ranking Members Connolly and Raskin, and other distinguished Members of the Subcommittees. I am Megan Tinker, Senior Advisor for Legal Review in the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS or the Department). Thank you for inviting me to discuss improper payments and the need for national Medicaid data to strengthen the program.

Created by statute in 1976, OIG is an independent body of auditors, evaluators, and investigators, deployed across the Nation, to help assess and protect the integrity of the Department's programs enacted by Congress. We remain committed to working with our stakeholders to achieve our shared goals of protecting beneficiaries and the taxpayer-funded programs they rely on from fraud, waste, and abuse, and promoting efficient and effective program operations.

Protecting Medicaid from fraud, waste, and abuse is an urgent priority because of its impact on the health and welfare of millions of Americans and on Federal and State spending. OIG has an extensive body of work examining vulnerabilities in Medicaid and recommending improvements to address high improper payments, the lack of program integrity safeguards, and health and safety concerns. Key to addressing each of these critical issues is robust, national Medicaid data that are complete, accurate, and timely.

In fiscal year (FY) 2016, Medicaid served more than 69 million enrollees at a cost of $574 billion. Medicaid serves more people than any other Federal health care program and represents one-sixth of the national health care economy. To ensure that Medicaid can continue to serve our Nation's most vulnerable populations well into the future, we must foster sound financial stewardship. Reducing improper payments is a critical element in protecting the financial integrity of Medicaid. Although not all improper payments are fraud – or even overpayments – all improper payments pose a risk to the financial security of these programs.

In FY 2016, estimated improper Medicaid payments totaled more than $36 billion. The Centers for Medicare & Medicaid Services (CMS) must do more to ensure States pay the right provider, the right amount, for the right service, on behalf of the right beneficiary. My testimony addresses those concepts within the framework of OIG's core program integrity principles of prevention, detection, and enforcement—highlighting the importance of high-quality Medicaid data for program integrity across all three principles.

Program Integrity Principles
Prevent – Know Who You Are Doing Business With
Detect – Identify Fraud, Waste, and Abuse in a Timely Manner
Enforce – Take Appropriate Action to Correct Problems, and Prevent Future Harm

Prevention: **State Medicaid programs do not always effectively screen providers or correctly determine beneficiary eligibility.**

The most effective way to prevent improper payments and fraud in Medicaid is to keep bad actors and ineligible beneficiaries out of the program to begin with. Complete and reliable data can help States do this. Without it, States may not know with whom they are doing business.

States have not fully enacted enhanced provider screening.

To ensure that Medicaid pays the right provider, the program must be able to identify the providers with whom it is doing business and keep bad actors out of the program. Preventing bad actors from entering the Medicaid program not only reduces improper payments, but also prevents the potential for patient harm.

States are required to screen providers according to the risk for fraud, waste, and abuse that they pose to Medicaid. However, States face challenges in meeting requirements to screen high-risk providers, including conducting fingerprint-based criminal background checks and site visits. Previous OIG work found that many States had yet to complete fingerprint-based criminal background checks and site visits. OIG made recommendations to CMS to assist States with completing these activities. CMS concurred with OIG's recommendations and has provided assistance to States. However, CMS continues to extend the deadline for completion of fingerprint-based criminal background checks, indicating that States are still working on provider enrollment. OIG has ongoing work to provide a status update on implementation of fingerprint-based criminal background checks.

It is important that CMS ensure that States timely and fully implement these critical safeguards, as even a single bad actor could defraud Medicaid of millions of dollars and endanger beneficiaries. For example, in Virginia, two individuals conspired to defraud a special caregiver program covered under Medicaid by submitting timesheets for payment for services that were never rendered. This scheme took place while one of the individuals was incarcerated. A State criminal background check could have revealed that one of the individuals had been convicted and might have helped prevent this fraud scheme.

In another example, in North Carolina, a mental health facility operator submitted fraudulent claims to Medicaid seeking reimbursement for services that were never provided to beneficiaries with developmental disabilities. The operator submitted at least $2.5 million in fraudulent claims using stolen beneficiary information from a defunct company that he previously co-owned, and received more than $2 million in reimbursements from Medicaid. State site visits could have revealed that the beneficiaries whose identities had been stolen from the defunct company were not actually receiving services.

These cases exemplify why OIG recommends that **CMS should improve provider screening by working with States to implement fingerprint-based criminal background checks and site visits for high-risk providers.**

It is important to know with whom Medicaid is doing business, not only to prevent improper payments to ineligible providers, but also to protect beneficiaries. OIG has raised concerns about the varying standards, and in some cases, minimal vetting, for Medicaid personal care services (PCS)

providers. This leaves the Medicaid program vulnerable to financial fraud. Even more concerning, it leaves Medicaid patients vulnerable to abuse and neglect. For example, an elderly woman in Idaho was hospitalized to treat malnutrition and dehydration because the caregiver failed to provide water and food. Suspecting she was a victim of neglect, investigators served a search warrant and found that she had been living in filth despite the fact that Medicaid was paying a PCS attendant to care for her everyday needs. **OIG continues to recommend that CMS establish minimum Federal qualifications and screening standards for all PCS attendants.**

For provider screening to be truly effective, States need timely, complete, and accurate data to efficiently and effectively identify the providers with whom they are doing business. To that end, OIG has issued several recommendations to CMS aimed at the development of a central repository or "one-stop shop" with provider information that all States and Medicare can use. This could reduce data-collection duplication and burdens on States and providers and improve the completeness and accuracy of the data available to Medicaid, the Children's Health Insurance Program (CHIP), and Medicare. The President's FY 2019 Budget request includes a proposal to consolidate provider enrollment screening for Medicare, Medicaid, and CHIP.

States are not always correctly determining Medicaid eligibility for beneficiaries.

Correctly determining beneficiary eligibility is vital to the accuracy of Medicaid payments. To ensure that Medicaid makes payments on behalf of the right beneficiary, it is critical to determine whether the beneficiary receiving services is actually eligible for Medicaid. Recent OIG audits of three States estimated that more than $1.2 billion in Federal Medicaid payments have been made on behalf of

potentially ineligible and ineligible beneficiaries. Lack of enrollment data systems functionality was a key contributor to these payments.

OIG recently reviewed whether certain States were correctly determining eligibility, following changes made by the Affordable Care Act (ACA) to Medicaid eligibility rules. ACA allowed States to expand Medicaid eligibility for certain low-income adults and claim a higher Federal Medical Assistance Percentage for those who are newly eligible under the expansion. As a result of States incorrectly determining beneficiaries' eligibility, payments made on behalf of these beneficiaries could be incorrect, resulting in the shift of costs from the State to the Federal Government. OIG reviews of Medicaid eligibility determinations by California, New York, and Kentucky reveal that these States did not comply with Federal and State requirements to verify applicants' income, citizenship, identity, and other eligibility criteria. In total, across these three States, OIG estimated that more than $580 million in Federal Medicaid payments were made on behalf of 183,579 potentially ineligible beneficiaries, and about $655 million in payments made on behalf of 413,349 ineligible beneficiaries—over $1.2 billion in total for more than 596,000 beneficiaries. Both human and system errors contributed to these payments, with some enrollment data systems lacking the ability to (1) deny or terminate ineligible beneficiaries; (2) properly redetermine eligibility when a beneficiary aged out of an eligibility group; (3) maintain records, per Federal requirements, relating to eligibility determinations and verifications; and (4) retrieve and use information from other Government databases, such as those managed by the Social Security Administration and Department of Homeland Security.

To ensure compliance with Federal and State requirements for determining Medicaid eligibility, we recommended that States ensure that enrollment data systems are able to verify eligibility criteria, develop and implement written policies and procedures to address vulnerabilities, and undertake redeterminations as appropriate.

Detection: Complete and reliable national Medicaid data are necessary for effective program oversight and management and to detect bad actors.

Proper oversight includes the capacity to detect problems in real time. This can help prevent improper payments, protect patients, and reduce time-consuming and expensive "pay and chase" activities. Detecting problems is a shared responsibility for all actors in the Medicaid program: CMS, States, managed care contractors, and providers. The lack of national Medicaid data hampers the ability to quickly detect improper payments, fraud, waste, or quality concerns, both within States and across the Nation. Unscrupulous providers committing fraud or engaging in patient harm do not respect State boundaries.

CMS must ensure the completeness and reliability of data in the Transformed Medicaid Statistical Information System.

Through the Balanced Budget Act of 1997, Congress mandated that States submit data to provide for a national Medicaid dataset. The Transformed Medicaid Statistical Information System (T-MSIS) is a joint effort by CMS and the States to address previously identified problems with national Medicaid claims and eligibility data. CMS's goals for T-MSIS are to improve the completeness, accuracy, and timeliness of Medicaid and CHIP data.

CMS began testing T-MSIS with 12 volunteer States starting in 2011 as a means to replace the Medicaid Statistical Information System as an enhanced national Medicaid dataset, after which CMS set a goal of having all States submit T-MSIS data by July 2014. CMS subsequently extended that deadline several more times. After multiple missed implementation deadlines, technological problems, competing priorities, and other implementation delays, as of last month 49 States and the District of Columbia had begun reporting data to T-MSIS.

As CMS and States continue to work toward full implementation, the completeness and reliability of T-MSIS data must be a top priority. A quality national Medicaid dataset is essential to States' and the Federal Government's ability to effectively and collaboratively administer and ensure the integrity of Medicaid. Fraud schemes affecting multiple States are very difficult to detect without comprehensive national data. Localized schemes can also be harder to detect without national data. Utilization or spending patterns may not appear problematic until compared against another State's experience or national averages. Recognizing such schemes in one State can alert other States to indicators of fraudulent or abusive practices that may be occurring in their jurisdiction. This information can lead to referrals to State law enforcement agencies like the State Medicaid Fraud Control Units or joint investigations across State lines. For example, it is important for CMS to ensure that the same data elements are being consistently reported across States, are uniformly interpreted across all States, and that those actually being reported will best inform program management and oversight. To accomplish this, OIG recommends that **CMS establish a deadline for when national T-MSIS data will be available**

for multi-State program integrity efforts. Without a fixed deadline, some States and CMS may not make the full implementation of T-MSIS a management priority.

CMS Should Ensure That States Report Encounter Data for All Managed Care Entities.

Managed care encounter data are among the most critical to be included in T-MSIS. Approximately 80 percent of all Medicaid beneficiaries receive part or all of their services through managed care. State Medicaid agencies contract with managed care entities to deliver health services and perform certain administrative functions, such as data collection and reporting. Most importantly, managed care entities are required to report medical claims data, known as encounter data, to States that then report the data to CMS via T-MSIS. Encounter data include detailed information about the services provided to Medicaid beneficiaries enrolled in managed care. Like Medicaid claims for services provided on a fee-for-service basis, encounter data are the primary record of services provided to Medicaid beneficiaries enrolled in managed care. The Society of Actuaries calls encounter data "the single most important analytical tool for health plans and health programs. Without accurate and timely data, it is not possible to analyze costs, utilization or trends; evaluate benefits; or determine the quality of services being provided."

However, previous work by OIG found that States' Medicaid managed care encounter data were incomplete. Reasons that States cited for their failure to report complete information included the inability to collect encounter data from some managed care entities and limitations in the State's data systems. CMS has made progress in addressing this problem, including regulatory requirements, guidance, and an ongoing data quality monitoring review of submissions of encounter data through

T-MSIS. However, more must be done to ensure that the data necessary to provider program integrity in Medicaid managed care are complete, accurate, and timely. As a result, **we continue to recommend that CMS ensure that States report encounter data for all managed care entities.**

Enforcement: The lack of quality national Medicaid data hampers enforcement efforts.

Complete and reliable data are critical to identifying improper payments and to Federal and State enforcement efforts to keep fraudulent and harmful providers out of Medicaid and hold bad actors accountable.

National Medicaid data holds the promise of supporting and amplifying enforcement efforts. We have seen this potential realized in Medicare. For example, in July 2017, OIG and its law enforcement partners conducted the largest National Health Care Fraud Takedown in history. Sophisticated data analytics were critical. The end result—charges against more than 400 defendants across 41 Federal districts for their alleged participation in health care fraud schemes involving about $1.3 billion in false billings—protected the programs and sent a strong signal that theft of taxpayer funds will not be tolerated. Notably, 120 defendants, including doctors, were charged for their roles in prescribing and distributing opioids and other dangerous narcotics, and 295 providers were served with exclusion notices for conduct related to opioid diversion and abuse. A concurrent data brief underscored the magnitude of the problem by identifying concerns about extreme use and questionable prescribing of opioids in Medicare Part D. That is the power of data— leveraged by skilled auditors, investigators, and analysts—to protect the program and bring bad actors to justice.

Unfortunately, we cannot replicate this type of analysis and enforcement action in Medicaid. Despite CMS's progress in implementing T-MSIS, we presently lack national Medicaid data that are complete and comparable across States. Decreased improper payments and savings achieved through improved program integrity could provide funding for increased services and assessments of the value of these services to a larger number of beneficiaries.

Conclusion

OIG continues to identify effectively overseeing Medicaid as a top management challenge for HHS. Challenges include longstanding program integrity vulnerabilities, such as the limitations in national Medicaid data that make it more difficult to detect and address improper payments and fraud. Quality national Medicaid data allow for the transparency necessary to determine whether Medicaid is paying the right provider, the right amount, for the right service, on behalf of the right beneficiary. Data can help accelerate enforcements efforts, reduce costs, improve quality of care, and identify best practices. While CMS and States have made important strides to improve Medicaid data, it remains to be seen whether T-MSIS will live up to its potential. Ultimately, T-MSIS will be only as useful as the data it receives. This is why CMS must ensure the completeness and reliability of T-MSIS data and improve provider enrollment data to prevent unscrupulous providers from gaining entry to Medicaid. Such data are essential to the efficiency, effectiveness, and integrity of Medicaid regardless of how it is structured.

As a modern OIG, we are using data and technology in innovative ways to enhance and target our oversight efforts. By leveraging advanced data analytic techniques to detect potential vulnerabilities

and fraud trends, we are better able to target our resources to those areas and individuals most in need of oversight. Quality Medicaid data are key to replicating these successes for Medicaid program integrity efforts. While neither CMS nor State Medicaid agencies presently have the data necessary to support a 21st century Medicaid program, we believe this Committee's continued oversight will help ensure the high-quality data needed for a well-functioning Medicaid program. Thank you for the opportunity to testify on this important topic.