STATEMENT OF

KIM BRANDT,

DEPUTY ADMINISTRATOR & CHIEF OPERATING OFFICER

CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

"PROTECTING PATIENTS AND SAFEGUARDING TAXPAYER DOLLARS: THE ROLE OF CMS IN COMBATTING MEDICARE AND MEDICAID FRAUD"

BEFORE THE

U. S. HOUSE COMMITTEE ON ENERGY & COMMERCE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

MARCH 17, 2026

U.S. House Committee on Energy & Commerce,
Subcommittee on Oversight & Investigations
"Protecting Patients and Safeguarding Taxpayer Dollars: The Role of CMS in Combatting Medicare and Medicaid Fraud"
March 17, 2026

Chairman Joyce, Ranking Member Clarke, and members of the Subcommittee, thank you for the invitation and the opportunity to discuss ongoing efforts at the Centers for Medicare & Medicaid Services (CMS) to crush fraud, waste, and abuse in Medicare, Medicaid, and the Children's Health Insurance Program (CHIP). The number one priority at CMS is to preserve Medicare, Medicaid, and CHIP for the most vulnerable. Fraud in the health care system undermines trust, diverts critical resources, and harms patients and taxpayers alike. Fraud is not only a financial offense — it is a moral one.

Fraud can take many forms. A dishonest supplier bills Medicare for equipment never delivered. A bad actor recruits beneficiaries at community centers, offering small gifts in exchange for Medicare numbers that are later used to submit false claims. In more sophisticated schemes, organized criminal networks create entire sham clinics to siphon funds from federal programs.

When fraudsters bill for phantom services, they pollute medical records and erode public trust. A beneficiary's file might show that a wheelchair was delivered, making it harder for the beneficiary to obtain one when it is truly needed. It might list diagnostic tests that were never performed, confusing future providers. In some cases, fraudulent providers perform unnecessary procedures to justify billing, exposing patients to real physical harm.

Medicare and Medicaid are lifelines for seniors, people with disabilities, and low-income families. In Fiscal Year (FY) 2026, over 170 million Americans will rely on the programs CMS administers or oversees. Every dollar diverted to a fraudulent claim is a dollar unavailable for legitimate care like preventive screenings, mental health services, rural hospitals, home health visits, and lifesaving medications. CMS is not just a payer of claims, we are a steward of public trust. Our responsibility goes beyond balancing accounts; it must protect beneficiaries from exploitation and safeguard the integrity of programs that support nearly half the nation.

Comprehensive Regulations to Uncover Suspicious Healthcare (CRUSH) Initiative

That's why CMS has launched a new era of integrity with modern tools, tighter oversight, and unrelenting enforcement. Central to this modernization effort is CMS's commitment to engaging stakeholders and soliciting innovative solutions from the broader health care and technology communities. On February 25, CMS issued a Request for Information (RFI)[1] seeking stakeholder input on additional ways the agency can tackle fraud prevention and detection to help inform the development of a possible future rule under CMS' Comprehensive Regulations to Uncover Suspicious Healthcare (CRUSH) initiative. Stakeholders are encouraged to provide input on both existing authorities and ideas for new regulatory approaches.

Responses to this RFI will help inform CMS's strategic priorities, technology investments, and policy decisions moving forward as we implement our broad strategy to combat fraud, waste, and abuse through data-driven prevention and real-time enforcement.

[1] The RFI is available at: https://www.federalregister.gov/public-inspection/2026-03968/request-for-information-comprehensive-regulations-to-uncover-suspicious-healthcare

In 2025, CMS made significant progress in its fight to crush fraud, including:

- Suspending $5.7 billion in suspected fraudulent Medicare payments by leveraging advanced analytics, cross-agency coordination, and law enforcement partnerships;
- Preventing $1.5 billion in suspected fraudulent Medicare DMEPOS billing;
- Denying 122,658 Medicare claims for unnecessary items and services because they failed to satisfy Medicare's preliminary approval checks that confirm medical necessity and other coverage requirements;
- Revoking the ability of 5,586 providers and suppliers to bill the Medicare program due to inappropriate behavior;
- Sending 372 fraud referrals encompassing $3.7 billion in Medicare and Medicaid billing to law enforcement for potential legal action;
- Initiating a CMS-State Tax Fraud partnership with 28 states and the US Virgin Islands to strengthen state-federal enforcement against healthcare providers and suppliers who commit healthcare and tax fraud; and
- Working with states to ensure they return or provide additional documentation accounting for an estimated $1.8 billion in federal Medicaid funds that may have been spent on health care for individuals with an unsatisfactory immigration status.

Moving away from "Pay and Chase"

Historically, health care fraud enforcement often focused on recovering funds after an investigation revealed fraudulent payments. While recoveries remain important, CMS is committed to identifying and intercepting fraud before the funds leave our accounts, moving from a "pay and chase" strategy to a "caught and stopped" approach. To do this, CMS deploys advanced data analytics to detect suspicious billing patterns before payments are made. We screen providers before they are allowed to participate in Medicare, conduct audits, and collaborate with law enforcement to investigate and prosecute fraud. We educate beneficiaries on how to spot fraud or other suspicious billing and encourage them to report anything suspicious. We partner with states, insurers, and other federal agencies to share intelligence and close vulnerabilities.

At the heart of CMS's renewed focus on fraud prevention is the Fraud Defense Operations Center (FDOC), also known as the Fraud War Room, which integrates cross-functional expertise through a specialized team of data analysts, investigators, health policy experts, legal advisors, and law enforcement. The FDOC safeguards policyholders and protects taxpayer resources by leveraging rigorous data-driven analysis to proactively detect, address, and prevent fraud, waste, and abuse in real time.

In addition to the FDOC, the Trump Administration has taken aggressive action to curb the rampant fraud in Medicare and Medicaid. Dr. Oz and other senior CMS staff have traveled to multiple states to meet with governors, state tax authorities, Medicaid directors, and law enforcement officials to promote stronger state–federal collaboration. These visits have focused on data sharing, joint enforcement strategies, and using state tax investigations as a faster pathway to hold fraudulent providers accountable. By engaging directly with state leaders and frontline investigators, Dr. Oz has sought to reinforce a coordinated "crush fraud" strategy—one that leverages every available tool and partner to protect beneficiaries, safeguard taxpayer dollars, and restore public trust in CMS's federal health programs.

Collaboration with Law Enforcement and Federal Agencies

CMS works with its law enforcement partners who take a lead role in investigating and prosecuting alleged fraud. Since 2007, CMS has supported the Department of Justice's Health Care Fraud Unit's Strike Forces. A central component of the Health Care Fraud Unit Strike Forces is the use of advanced data analytics and interagency collaboration to identify, investigate, and prosecute fraudulent health care providers, shifting the focus to deterrence, recovery, and appropriate criminal sanctions for fraudulent actors. In 2025, CMS, along with the Health Care Fraud Unit's Data Analytics Team, HHS-OIG, and FBI announced that they were working closely together to create a Health Care Fraud Data Fusion Center to leverage cloud computing, artificial intelligence (AI), and advanced analytics to identify emerging health care fraud schemes. CMS complements those efforts by exercising its administrative authorities to protect Federal health care program dollars, including taking timely payment suspension actions when appropriate. We coordinate and deconflict with our law enforcement partners to ensure our actions do not interfere with ongoing investigations.

The Federal partners target areas with high incidence of fraud to carry out synchronized efforts to reduce fraud and recover taxpayer dollars. Together, activities like CMS' enhanced provider screening and fraud prevention activities; HHS-Office of Inspector General's (OIG) investigative, audit, evaluation, and data analytic work; and the Department of Justice's investigative and prosecutorial actions, root out existing fraud and abuse while acting as a deterrent for potential future bad actors. For example, in the 2025 National Health Care Fraud Takedown, the Justice Department charged 324 defendants with over $14.6 billion in false claims, and CMS announced that it successfully prevented over $4 billion from being paid, as well as suspending or revoking the billing privileges of 205 providers in the months leading up to the Takedown.

CMS also relies on the Department of the Treasury's Do Not Pay (DNP) system as part of its improper payment and eligibility screening framework. Consistent with the Payment Integrity Information Act, CMS screens certain payment and award data against DNP's centralized data sources—such as the Death Master File and exclusion records—and incorporates these checks into its payment integrity processes. Treasury's DNP Program also serves as the technical service provider for the Public Assistance Reporting Information System (PARIS), a data matching program that helps states identify individuals who may be receiving public assistance benefits across multiple states or programs and supports death data matching to reduce improper enrollments.

Provider Enrollment

Strong provider enrollment is the first line of defense against health care fraud. By thoroughly screening and verifying providers before they can bill Medicare—through background checks, site visits, and risk-based reviews—CMS helps ensure that only legitimate, qualified entities can access federal health care funds. As of March 2026, there are 2,979,803 providers and suppliers enrolled in the Medicare Fee-For-Service (FFS) program.

Enhanced screening tools include fingerprint-based criminal background checks for high-risk providers and suppliers, unannounced site visits, license verification, database cross-checks, and ownership disclosure requirements. In Medicare, CMS uses the Provider Enrollment, Chain, and Ownership System (PECOS) to collect and store records for all Medicare provider and supplier enrollment data across Part A and Part B. This system streamlines the enrollment process by enabling healthcare providers and suppliers to digitally submit and manage their Medicare enrollment information. The Advanced Provider Screening (APS) system provides a more sophisticated layer of protection. APS is an interactive screening, monitoring, and alerting system that identifies ineligible providers and houses a centralized provider repository of criminal activity, licensure status, and identity information. In Medicaid, the Data Exchange (DEX) system facilitates the sharing of provider termination and revocation data among CMS and state programs, maintaining a centralized repository accessed by all 50 states, the District of Columbia, and Puerto Rico.

Leveraging Technology and Data Integration

Recent CMS efforts have increasingly emphasized sophisticated data analytics. By linking Medicare and Medicaid claims data, provider ownership information, pharmacy records, and external data sources, CMS can identify patterns that might otherwise go undetected. In addition, AI and machine learning tools enhance anomaly detection, allowing CMS to continuously refine risk models. The Fraud Prevention System (FPS) uses advanced data analytics and predictive modeling to identify aberrant billing patterns in real time. By analyzing millions of claims daily, FPS flags suspicious behavior—such as unusual billing spikes, improbable service combinations, or geographic anomalies—allowing CMS to intervene before funds are disbursed. This approach not only protects taxpayer dollars but also reduces the risk that fraudulent or unnecessary services will be provided to beneficiaries.

Crushing Fraud Chili Cook-Off Competition

CMS is committed to strengthening our efforts in this area. Last fall, CMS held the Crushing Fraud Chili Cook-Off Competition and invited companies to submit their best tech recipes for crushing fraud. The Cook-Off was a market-based research challenge aimed at harnessing explainable AI, specifically machine learning models, to detect anomalies and trends in Medicare claims data that can be translated into novel indicators of fraud. This challenge sought innovative, scalable technologies that reduce labor-intensive processes while keeping humans meaningfully in the loop to ensure effective oversight and interoperability. CMS invited research proposals from all interested parties and reviewed over 259 applications during the first phase of the competition. For the second and final phase, CMS provided ten finalists with access to CMS's Limited Data Set of Medicare Hospice, Part B, and Durable Medical Equipment (DME) claims data. Participants applied their proposed techniques to the data and submitted a summary of their findings, as well as proposed scalable analytic and policy solutions. On December 15th, CMS selected Milliman, Inc. as the winner of the Chili Cook-Off Competition. The insights and tools developed through this competition will guide us as we implement new capabilities and technologies to crush fraud and protect taxpayer dollars.

Guarding Beneficiary Information

Health plans use confidential member IDs for transactions like health care billing, eligibility status, and claim status. Individuals committing health care fraud are increasingly stealing Medicare Beneficiary Identifiers (MBIs) and other member IDs in various ways, such as deceiving patients, hacking into health care organizations' systems, or misusing online lookup tools. Once member IDs are stolen, they are used to submit fraudulent claims to Medicare, Medicaid, and other health insurance companies.

IDea

CMS hosted the IDea Challenge last December, bringing together 78 attendees from technology, government, and health care sectors to address member ID and MBI theft and misuse. During two events, participants worked in teams to identify the most serious problems with member ID theft and misuse and pitch their ideas on how to solve them. The top-voted concepts emphasized limiting the damage from compromised credentials by transitioning from static identifiers (such as MBIs or NPIs) to transaction-based or per-provider unique tokens; verifying provider identities in real-time through biometrics and digital credentials; and engaging beneficiaries through real-time alerts and mobile apps. These proposals aim to create a more secure Medicare system by empowering both providers and beneficiaries to actively prevent fraud.

CMS-State Tax Fraud Partnership

Health care providers and suppliers who bill fraudulent insurance claims often fail to report the associated income on their tax returns. This creates a dual-layered crime—one that drains both federal healthcare programs and state tax systems. CMS invited states and territories to collaborate in a joint effort between CMS and state tax authorities to identify and take action against providers and suppliers who commit both health care and tax fraud. This initiative leverages the fact that state tax fraud prosecutions are often faster than traditional health care fraud cases, and criminal tax fraud convictions enable CMS to swiftly revoke billing privileges. To date, 32 of the 44 states and territories with income taxes have expressed interest in partnering with CMS on the fraud tax project. In previous partnerships, similar approaches led to the identification and prosecution of 12 Medicare providers and suppliers who had received fraudulent payments but failed to report the income. More recently, participating states reviewed 300 suspect Medicare providers and suppliers and found 32 with unreported earnings exceeding $2 million each, underscoring the effectiveness of coordinated data sharing and investigative efforts.

Medicaid Eligibility and Enrollment

Since 2009, CMS has required states to conduct interstate matching via the Public Assistance Reporting Information System (PARIS) to confirm that beneficiaries are not enrolled in Medicaid or CHIP programs across multiple states. In 2025, CMS conducted a data analysis and found that a significant amount of concurrent enrollment existed in 2024. CMS identified an average of 1.2 million Americans each month were enrolled in Medicaid/CHIP in two or more states and an average of 1.6 million Americans each month were enrolled in both Medicaid/CHIP and a subsidized Exchange plan. These concurrent enrollments may have resulted in an estimated $14 billion in waste annually. CMS is partnering with states to systematically identify and address concurrent enrollments across Medicaid and CHIP programs. Further, CMS is working to implement new requirements in Public Law 119-21, which CMS refers to as the "Working Families Tax Cut" (WFTC) legislation, designed to eliminate and prevent duplicate enrollment in Medicaid programs.

In addition, audits conducted by the HHS OIG have shown that states have faced challenges with identifying and preventing payments from being made on behalf of individuals who are deceased. Thanks to the WFTC law, beginning January 1, 2027, states will be required to check the Social Security Administration's Death Master File (DMF) on at least a quarterly basis to identify any Medicaid enrollees who are deceased. States will be required to treat such information as factual, and following the required provision of notice and fair hearing rights, disenroll such individuals from Medicaid without requesting additional information from the household or authorized representative. CMS is committed to working with states as they prepare to implement this new requirement. States will also be required to check the DMF quarterly to ensure deceased providers do not remain enrolled in Medicaid.

Targeted, Risk-Based Approaches

CMS uses a targeted, risk-based approach to finding and crushing fraud so we can focus our oversight resources where they will have the greatest impact. By analyzing claims data, billing patterns, provider characteristics, geographic trends, and prior enforcement history, CMS identifies service lines, provider types, or regions that present elevated risk of improper payments or beneficiary harm. This allows the agency to apply enhanced screening, prepayment review, prior authorization, or focused audits to high-risk areas rather than burdening all providers with unnecessary oversight. A risk-based strategy improves efficiency and reduces administrative burden on compliant providers and enables CMS to intervene earlier, providing stronger protection for beneficiaries and taxpayer dollars.

Hospice in Medicare Fee-for-Service

Hospice care provides an invaluable service to patients and families during life's most difficult moments, offering comfort, dignity, and compassionate end-of-life support when it matters most.

Unfortunately, CMS research has revealed that some hospices are exploiting Medicare's per-diem payment policies and using the sensitivity surrounding end-of-life care to profit from fraud at the expense of beneficiaries through fraudulent enrollment of ineligible patients, billing for services never provided, or extending care beyond medical necessity. In response to these findings, CMS revisited and revitalized our hospice program integrity strategy, focusing on identifying bad actors and addressing fraudulent activity to minimize impacts to beneficiaries in the Medicare program. As part of this strategy, CMS embarked on a nationwide hospice site visit project, making unannounced site visits to every Medicare-enrolled hospice to verify operational status and ownership information, adequate staffing, and key medical record documentation. As a result of this effort, 48 hospices have had their Medicare enrollment revoked. An additional 478 hospices have had their Medicare billing privileges deactivated, meaning they are unable to bill Medicare, and 318 hospices updated their practice locations to reflect address changes. CMS also streamlined the hospice disenrollment process for Medicare beneficiaries.

In addition, based on numerous reports of hospice fraud, waste, and abuse in Arizona, California, Nevada, and Texas, CMS implemented a provisional period of enhanced oversight (PPEO) for newly enrolling hospices in those states, and is conducting expanded prepayment reviews and related activities for existing hospices. Through December 2025, 817 hospices have been subject to medical review. CMS has revoked the Medicare enrollment of 181 of these hospices. Further, CMS has expanded its PPEO and other high-risk prepayment review efforts to include hospices in GA and OH beginning in 2026.

Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS)

In February, CMS announced that we are taking decisive steps to prevent fraudulent Medicare billing by durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) companies. A six-month nationwide moratorium on new Medicare enrollment for certain DMEPOS suppliers builds on CMS's stopping more than $1.5 billion in suspected fraudulent billing in this area last year. The DMEPOS supplier enrollment moratorium will allow CMS to explore additional safeguards to further mitigate longstanding instances of fraud, waste, and abuse perpetrated by certain DMEPOS companies. It applies to all medical supply companies that are seeking initial enrollment and medical supply companies that engage in a change of majority ownership that triggers our 36-month rule[2].

CMS also plans to publish information on providers/suppliers whose participation in the Medicare program has been revoked, including their National Provider Identifier and the reason for the revocation. This additional transparency will allow patients and payers, including private insurers, to understand which providers have been subject to such administrative enforcement action by the government.

Moving Forward

CMS's evolving fraud prevention strategy represents a fundamental shift from reactive detection to proactive prevention, emphasizing the need to stop fraud before payments are made rather

[2] The 36-month rule is triggered when an individual or organization acquires more than a 50 percent direct ownership interest in a DMEPOS supplier during the 36 months following the DMEPOS supplier's initial enrollment into the Medicare program or the 36 months following the DMEPOS supplier's most recent change in majority ownership (including asset sale, stock transfer, merger, and consolidation). This includes an individual or organization that acquires majority ownership in a DMEPOS supplier through the cumulative effect of asset sales, stock transfers, consolidations, or mergers during the 36-month period after Medicare billing privileges are conveyed or the 36-month period following the DMEPOS supplier's most recent change in majority ownership. Some narrow exceptions apply (e.g., A DMEPOS supplier's parent company is undergoing an internal corporate restructuring, such as a merger or consolidation). See 42 CFR 424.551.

than recovering funds after the fact. This forward-looking approach includes expanding advanced data analytics and artificial intelligence (AI) tools to detect anomalous billing in real time, strengthening provider enrollment screening and affiliation disclosure requirements, and applying targeted, risk-based oversight in high-vulnerability areas such as hospice and durable medical equipment.

CMS is strengthening collaboration across the fraud-fighting ecosystem—partnering with federal and state agencies, law enforcement, private insurers, and technology vendors to share intelligence, close enforcement gaps, and create a unified defense against increasingly sophisticated fraud schemes. CMS also recognizes that certain large-scale fraud schemes can have broader national security implications, particularly when carried out by organized or transnational actors, reinforcing the need for coordinated and intelligence-informed safeguards. By combining cutting-edge analytics with human expertise and multi-stakeholder coordination, CMS aims to build a more resilient system that adapts quickly to emerging threats, deters would-be fraudsters through swift consequences, and preserves program integrity without burdening legitimate providers with unnecessary administrative hurdles.

By fostering transparency, soliciting feedback, and remaining open to new approaches, CMS is building a fraud prevention framework that is not only more effective but also more responsive to the realities facing providers, beneficiaries, and the rapidly changing healthcare environment. CMS will continue working with Congress and stakeholders across the health care industry to implement and build on the tools provided by the WFTC legislation. Together, we can close enforcement gaps, protect state and federal resources, and ensure that taxpayer dollars go where they are intended— to patient care, not criminal gain.