U.S. Department of Health and Human Services

Office of Inspector General

WHITE PAPER

August 2026 | OEI-02-24-00311

The Nation's Challenge to Combat Durable Medical Equipment Fraud in Medicare

HHS Office of Inspector General
HIGHLIGHTS

August 2026 | OEI-02-24-00311

White Paper: The Nation's Challenge to Combat Durable Medical Equipment Fraud in Medicare

Each year, bad actors defraud Medicare and taxpayers of millions of dollars by billing for durable medical equipment that enrollees do not need or never receive. Despite efforts to combat this fraud, bad actors continually devise new schemes. **Bold action is needed to address the underlying problems that allow durable medical equipment fraud to persist.**

CMS has recently taken steps to increase its fraud-fighting efforts. For example, CMS has created a new Fraud Defense Operations Center to more proactively identify suspect billing and suspend payments.[1] However, given the extent of durable medical equipment fraud in Medicare and the continuously evolving nature of durable medical equipment fraud schemes, more specific attention is needed to understand and prevent this type of fraud.

This white paper presents actions that CMS and others can take to stop bad actors from exploiting Medicare. It focuses on three elements that bad actors need to commit fraud: a Medicare-enrolled supplier, a physician order, and an enrollee identification number.

Elements Needed to Commit Fraud	Fraud Method	Calls to Action to Combat Fraud
Medicare-enrolled supplier Before a supplier is permitted to bill Medicare, it must enroll in the program.	Bad actors are **evading enrollment safeguards**, e.g., by hiding the owner's true identity.	**Block fraud at the front door by strengthening Medicare enrollment.** ○ Improve detection of **unreported changes of ownership and straw owners**; and ○ Increase **oversight of newly enrolled** suppliers.
Physician orders To bill Medicare, suppliers must have physician orders verifying that the enrollee needs the equipment or supply.	Bad actors are **creating—or paying for—fake physician orders** and using them to submit fraudulent claims.	**Catch fake physician orders and claims to stop fueling fraud.** ○ **Engage ordering physicians** in fraud-fighting efforts; and ○ **Harness new technologies and analytic tools** to better detect and stop payments for fraudulent claims.
Medicare enrollee identification numbers Suppliers need enrollee identification numbers to bill Medicare.	Bad actors are **stealing or purchasing stolen Medicare enrollee identification numbers** to submit fraudulent claims.	**Stop the use of stolen enrollee identification numbers to shut down fraud.** ○ **Partner with social media companies** to prevent the sale of enrollee numbers on their platforms; and ○ **Change the way Medicare protects** enrollee identification numbers.

Introduction: Durable Medical Equipment Fraud in Medicare

Each year, bad actors defraud Medicare and taxpayers of millions of dollars by billing for durable medical equipment that enrollees do not need or never receive. In some instances, they trick Medicare enrollees into sharing their personal information and then use it to bill Medicare. In other instances, they pay physicians to sign fake orders for patients they have never even met. Commonly, these bad actors—including some operating from outside the country—use straw owners to hide their true identities and evade oversight. **This fraud must be stopped.**

Durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) include items such as wheelchairs, knee braces, and diabetic testing strips that allow Medicare enrollees to manage an illness or injury.

To address DMEPOS fraud, the Centers for Medicare & Medicaid Services (CMS) recently implemented a number of additional safeguards. Notably, CMS is working with the Office of Inspector General (OIG) through its new Fraud Defense Operations Center to more proactively identify suspect billing and suspend payments. CMS has also instituted a nationwide temporary moratorium on Medicare enrollment of new DMEPOS suppliers while it considers further safeguards.[4]

DMEPOS Fraud

Operation Gold Rush

A transnational criminal organization is accused of running a complex DMEPOS fraud scheme that billed Medicare for more than $10 billion.[2] The group used straw owners to hide their true identities while buying dozens of DMEPOS suppliers that were already allowed to bill Medicare. Using stolen enrollee information, they then submitted huge volumes of false claims for medical equipment that was never ordered by physicians and never provided to patients. See Appendix A for more information.

Operation Brace Yourself

Bad actors lured Medicare enrollees into calling overseas call centers with ads for free braces and then pressured them into accepting multiple unnecessary items.[3] The calls were passed to telemedicine physicians who ordered unneeded braces, and unscrupulous DMEPOS companies used those orders to bill Medicare. The bad actors used the proceeds from this fraud to purchase exotic automobiles, yachts, and luxury real estate.

Nonetheless, DMEPOS fraud continues to be a significant concern in Medicare. Bad actors continually devise new schemes to evade CMS's safeguards and commit fraud. In one case alone, bad actors are accused of fraudulently billing Medicare for over $10 billion in DMEPOS.[5] (See the text box for more information.)

This white paper presents actions that CMS and others can take to stop bad actors from exploiting the Medicare program. It draws on OIG's expertise from investigations, audits, and evaluations, as well as structured interviews with CMS staff, CMS contractors, and Medicare Advantage organizations.

The white paper focuses on three key elements that bad actors need to commit DMEPOS fraud:

1. a Medicare-enrolled DMEPOS supplier,
2. a physician order for DMEPOS, and
3. a Medicare enrollee's identification number.

For each of these elements, the paper describes how bad actors commit fraud, identifies existing vulnerabilities, and presents calls to action to address the underlying problems that allow fraud to persist.

Chapter 1: Becoming a Medicare-enrolled DMEPOS Supplier

FRAUD METHOD:

To commit DMEPOS fraud in Medicare, bad actors must first become a DMEPOS supplier that is enrolled in Medicare. CMS requires that DMEPOS suppliers enroll in Medicare before they are permitted to bill the program.[6]

There are two main ways that bad actors become DMEPOS suppliers that are enrolled in Medicare.

- **Open a new DMEPOS supplier business and enroll** it in Medicare.
- **Purchase an existing DMEPOS supplier that is already enrolled** in Medicare.

Fraud involving straw owners

The owner of a network of DMEPOS suppliers pled guilty for his role in a $39.5 million fraud scheme.[7] This individual listed straw owners on enrollment forms and bank accounts to conceal his involvement, paid kickbacks to obtain signed physician orders, and submitted claims for medically unnecessary orthotic braces.

SAFEGUARDS & VULNERABILITIES:

Despite current safeguards, bad actors are still able to become Medicare-enrolled DMEPOS suppliers.

- **On-site inspections do not always prevent bad actors from enrolling in Medicare.** When suppliers apply to enroll in Medicare, CMS conducts several screening checks, including on-site inspections.[8] These inspections focus on whether suppliers meet specific standards—such as posting their hours and having a working business phone number.[9] However, the timing of these on-site inspections can be predictable, allowing bad actors to temporarily stage their facilities to appear compliant.
- **Surety bonds are not effectively protecting the program against fraud.** Suppliers are required to purchase a surety bond, which is intended to deter fraud and ensure that CMS can recover overpayments.[10] Most DMEPOS suppliers are required to purchase a $50,000 surety bond—typically costing about $1,500—which has not kept bad actors from fraudulently billing Medicare.[11]
- **Straw owners are used to evade oversight.** CMS collects information about the owners of DMEPOS suppliers and conducts fingerprint-based background checks as a part of the enrollment process. However, bad actors sometimes hide the true

owners by using straw owners—also known as nominee owners—which evades these checks.

- **Unreported changes of ownership are difficult to detect.** CMS requires that DMEPOS suppliers report changes in majority ownership. However, CMS does not have a single data source to verify ownership information or detect unreported changes of ownership.[12] Instead, it must rely on multiple data sources, including State data, which is not always consistent or accurate.

- **Paper enrollment applications can be used to circumvent identity checks.** CMS allows DMEPOS suppliers to submit either paper or electronic enrollment applications. Bad actors can use paper applications to avoid certain identity checks that are required to access CMS's online enrollment system. Additionally, paper applications can conceal the location of the applicant, making it more difficult to track bad actors.

- **DMEPOS suppliers that bill only Medicare Advantage are not required to enroll in Medicare.** As a result, these suppliers are not subject to CMS's screening checks or other enrollment requirements and may pose an increased risk to the program.

CALLS TO ACTION:

Block fraud at the front door by strengthening Medicare enrollment

CMS has recently taken several steps to prevent bad actors from becoming DMEPOS suppliers that are enrolled in Medicare.[13] However, additional actions are needed.

These include:

- **Strengthen on-site inspections to prevent bad actors from enrolling in Medicare.** On-site inspections are critical to identifying and stopping bad actors from enrolling in Medicare. To make the inspections more effective, CMS should strengthen the criteria for on-site inspections. It should also target its approach by conducting more thorough or frequent on-site inspections of high-risk suppliers. This could include additional unannounced on-site inspections to ensure that bad actors cannot predict when site visits will occur.

- **Improve detection of unreported changes of ownership and straw owners.** Verifying ownership information can stop bad actors from evading oversight. CMS should work with its Federal partners, such as the Department of Treasury, to identify existing data or collect new data that could improve CMS's ability to track ownership. In the interim, CMS should strengthen its use of State-level ownership data by using artificial intelligence (AI) or other technologies on an ongoing basis to

identify changes of ownership that have not been reported to CMS. It could also more closely monitor instances of suppliers changing the bank accounts where their Medicare payments are deposited (i.e., their electronic fund transfer information), which may indicate that a supplier has a new owner or a straw owner.

- **Ban suppliers from using paper applications to circumvent oversight.** Requiring all DMEPOS suppliers to enroll using CMS's electronic application system is an important step to reduce DMEPOS fraud.[14] Electronic submissions require the supplier to obtain a login and can sometimes be traced to confirm who submitted the information, whereas paper submissions cannot.

- **Increase oversight of newly enrolled DMEPOS suppliers.** Newly enrolled DMEPOS suppliers and suppliers that recently changed ownership pose an increased fraud risk.[15] To address this risk, CMS should implement a period of enhanced oversight of newly enrolled DMEPOS suppliers and those that recently changed ownership.[16] This enhanced oversight would allow CMS to rapidly identify fraudulent suppliers and take appropriate actions in accordance with Section 1866(j)(3) of the Social Security Act.

- **Reassess and potentially update surety bond requirements to better deter fraud.** CMS's surety bond requirements—including the minimum surety bond amount (i.e., $50,000)—have not changed since the introduction of this requirement in 2009. Updating these requirements may better deter fraud. OIG has additional work on surety bonds underway, which will provide more information.[17]

- **Require all DMEPOS suppliers that bill Medicare Advantage to enroll in Medicare.** This action may require statutory change. It would ensure that all DMEPOS suppliers that bill Medicare Advantage undergo CMS's screening checks.[18] A forthcoming OIG issue brief discusses this topic in more detail.[19]

Bolder actions for consideration:

- **Take a different approach to enrolling DMEPOS suppliers.** CMS could explore alternative approaches to enrolling DMEPOS suppliers. Fraudulent DMEPOS suppliers can cluster in geographic areas, such as in parts of a State, certain zip codes, or even specific buildings. In these areas, it appears that there are far more DMEPOS suppliers than necessary to meet enrollee needs.

  To address this issue, CMS could consider requiring prospective suppliers to demonstrate that its participation in the Medicare program would help meet unmet enrollee needs within an area. Alternatively, CMS could consider denying enrollment to suppliers in areas without unmet enrollee needs. CMS should consult with

outside experts and other agencies to develop approaches that ensure enrollee needs are met while protecting the integrity of the Medicare program.

Chapter 2: Obtaining Physician Orders and Submitting Fraudulent Claims for DMEPOS

FRAUD METHOD:

To receive payment from Medicare, DMEPOS suppliers are required to obtain an order from a physician that documents the enrollee's need for the item or supply.[20] The supplier must enter the National Provider Identification (NPI) number of the ordering physician on the Medicare claim and retain the order and other supporting documentation in its records.

There are four main ways that bad actors obtain fake physician orders and submit fraudulent claims.

1. **Create fake orders** and other documentation to make it appear that the enrollee needs the DMEPOS items when they do not.
2. **Pay kickbacks** to physicians to order DMEPOS for enrollees. These physicians typically have little to no contact with the enrollees.
3. **Scam physicians into unwittingly signing orders** for unneeded DMEPOS for their patients, e.g., by faxing pre-filled orders for physicians to sign.
4. **Obtain stolen physician identification numbers** and use these identifiers to bill for DMEPOS without having an order.

Examples of fraud involving fraudulent physician orders

A Michigan physician was sentenced to 4 years in prison for her role in a $6 million fraud scheme.[21] She ordered thousands of medically unnecessary orthotic braces for patients over a 6-month period.

The owner of a DMEPOS supplier pled guilty to paying $3.7 million in kickbacks for fraudulent orders for DMEPOS items and fraudulently billing Medicare $51 million.[22]

SAFEGUARDS & VULNERABILITIES:

Despite current safeguards, bad actors still obtain fake physician orders and submit fraudulent claims.

- **Ordering physicians may not know that they are listed on fraudulent DMEPOS claims.** Physicians are not routinely notified when DMEPOS claims list them as the ordering physician. As a result, physicians may not be aware when their information has been stolen and used to create fake orders or submit fraudulent claims.
- **Data analysis does not always identify bad actors because fraud schemes constantly evolve.** CMS and its contractors conduct proactive data analyses of

claims data to identify unusual patterns that may indicate fraud and require follow-up, including further investigation or referral to law enforcement. However, bad actors adapt their fraud schemes to avoid these detection methods. For example, bad actors started purchasing lists of Medicare enrollees with the names of their physicians. They then listed the enrollee's own physician as the "ordering physician" on DMEPOS claims, which can evade CMS's detection efforts that look for the absence of a prior relationship between the enrollee and the ordering physician.

- **Medical reviews are mainly focused on reducing unintentional billing errors rather than fraud.** CMS contractors conduct medical reviews of a limited number of DMEPOS claims. For the past several years, CMS contractors have mainly conducted medical reviews that focus on educating suppliers about inappropriate billing.[23] These types of reviews help reduce billing errors but do not focus on reducing fraud.

- **Fake orders and documentation generated by AI are harder to detect.** As part of medical reviews, CMS contractors check physician orders and supporting documentation to determine if the DMEPOS was medically necessary. However, advancements in AI allow bad actors to quickly create, for each fraudulent claim, documentation that appears realistic and may be difficult to detect.

- **Payments from secondary payers—such as Medigap plans—may contribute to DMEPOS fraud.** CMS can suspend its payments to suppliers when fraud is suspected.[24] However, these suspensions do not apply to secondary payers. CMS's payment system is set up to pass supplier claims to secondary payers for payment. As a result, even if CMS suspends its payment, secondary payers may continue to pay potentially fraudulent claims.[25] This may increase health care costs for Medicare enrollees and other supplemental insurers, and may create incentives for bad actors to continue submitting fraudulent claims to Medicare even after CMS has initiated an investigation and suspended their payments.

- **Medicare Advantage organizations are not required to submit information to CMS about the physicians who order DMEPOS.** Identification numbers for physicians who order DMEPOS are an essential tool for safeguarding program integrity; however, a prior OIG report found ordering provider NPIs were largely missing from the Medicare Advantage data despite evidence that many Medicare Advantage organizations can, and do, already collect this information.[26]

CALLS TO ACTION:

Catch fake physician orders and claims to stop fueling fraud

CMS recently took a number of steps to prevent bad actors from obtaining fake physician orders and submitting fraudulent claims for DMEPOS.[27] However, additional actions are needed.

These include:

- **Engage ordering physicians in fraud-fighting efforts.** Physicians are critical partners in identifying and preventing fraudulent orders. CMS should pursue different ways to further engage physicians in the fight against fraud. CMS could develop an electronic verification method for physicians to confirm their orders before certain claims are paid. Alternatively, CMS could issue reports to physicians detailing the DMEPOS they ordered and request that physicians review the information and report any fraudulent billing to CMS or OIG. In addition, CMS should also continue to conduct outreach to ensure that ordering physicians are aware of DMEPOS scams and remain vigilant when signing orders.

- **Harness new technologies and analytic tools to better detect and stop payments for fraudulent DMEPOS claims.** Continuously integrating new technologies and analytic tools into oversight and monitoring is critical to ensure that detection methods evolve as fraud changes. CMS is currently using new technologies in its oversight and monitoring activities. As a part of these activities, CMS should explore the use of AI and other technologies to assist clinical experts who conduct medical reviews.[28] For example, CMS should explore whether AI-based technology could allow clinical reviewers to identify AI-generated orders and documentation.

- **Enhance the use of payment suspensions.** CMS recently increased its use of payment suspensions to address potential fraud. CMS should continue these efforts and identify opportunities to streamline the use of payment suspensions to better prevent fraudulent payments for DMEPOS. These efforts help to ensure that taxpayer dollars are not paid out to bad actors.

- **Expand medical reviews to prevent fraud.** Broadening the types of reviews that contractors routinely conduct would more effectively prevent fraudulent billing. CMS could provide contractors with more flexibility on the types of reviews they conduct. For example, contractors could focus on conducting pre-payment reviews of new suppliers. Further, CMS should ensure that contractors can review appropriate supporting documentation, such as proof of delivery.

- **Work with secondary payers to stop fraudulent billing.** Coordinating with secondary payers—and helping them prevent payments to bad actors—is key to deterring fraud. CMS recently began sharing payment suspension information with secondary payers to help them prevent payments to potentially fraudulent suppliers. It is important for CMS to assess whether this effort provides sufficient information to ensure that secondary payers can prevent payments to fraudulent suppliers and, if needed, take additional steps.

- **Require Medicare Advantage organizations to submit the identification number for the physicians who order DMEPOS.** OIG has previously recommended that CMS require Medicare Advantage organizations to report ordering provider NPIs on encounter data.[29] These numbers are critical pieces of data for preventing and detecting fraud and abuse.

Chapter 3: Obtaining and Using Enrollee Identification Numbers to Fraudulently Bill Medicare

FRAUD METHOD:

DMEPOS suppliers need enrollee identification numbers to bill Medicare for DMEPOS.

There are four main ways bad actors obtain these numbers.

- **Steal** enrollee identification numbers. This can occur when health care data systems are breached in a cyberattack.
- **Purchase** stolen enrollee identification numbers, e.g., on the dark web or social media platforms.
- **Scam** enrollees into unwittingly disclosing their identification numbers.
- **Improperly access** online lookup tools that allow providers and suppliers to find enrollees' identification numbers.

Fraud involving enrollee identification numbers

A Florida man was convicted for his role in a $109 million DMEPOS fraud scheme.[30] This individual worked with foreign call centers that tricked enrollees into revealing their personal information. He then sold this information to a DMEPOS supplier that used it to fraudulently bill Medicare.

SAFEGUARDS & VULNERABILITIES:

Despite current safeguards, bad actors are able to obtain and use stolen enrollee identification numbers.

- **Numerous cyberattacks** have targeted the health care industry and have led to large scale data breaches of enrollee identification numbers.
- **Enrollee lookup tools are improperly accessed by bad actors.** CMS has online tools that allow suppliers and providers to find an enrollee's identification number.[31] Bad actors are using authorized user accounts to steal large batches of enrollee identification numbers and then using these numbers to fraudulently bill Medicare or selling them to others seeking to fraudulently bill Medicare.
- **Bad actors make unsolicited contact** (via phone or text) with enrollees and convince them to disclose their identification numbers or personal information. In many cases, these bad actors are not working directly for DMEPOS suppliers. Instead, they

work as marketing agencies, call centers, or other third-party entities that sell the leads and information to DMEPOS suppliers.

- **Social media platforms and the dark web** are used to sell stolen identifiers.

CALLS TO ACTION:

Stop the use of stolen enrollee identification numbers to shut down fraud

CMS recently took several steps to prevent bad actors from obtaining and using stolen enrollee identification numbers.[32] However, additional actions are needed.

These include:

- **Discontinue or better protect enrollee lookup tools.** Online enrollee lookup tools create a significant fraud risk and allow bad actors to steal enrollee numbers. CMS should assess whether the lookup tools are needed and determine whether they can be discontinued and taken offline. If not, immediate action to further restrict access to the tools is needed. For example, CMS could restrict how many times a provider or supplier can access the tools each month or take other actions to prevent users from obtaining large batches of identification numbers at one time.

- **Prohibit DMEPOS suppliers from making all types of unsolicited contact with enrollees.** Currently, Federal law prohibits DMEPOS suppliers from making unsolicited phone calls to Medicare enrollees but does not expressly prohibit other types of contact, nor does it expressly prohibit entities associated with DMEPOS suppliers from making contact.[33] Entities that knowingly make unsolicited telephone contacts are subject to nonpayment of claims and exclusion from Federal health care programs. To help fight emerging DMEPOS fraud schemes, CMS should seek statutory changes to expressly extend the prohibition on unsolicited telephone contacts to other types of contact (e.g., text, email, and other digital means) and entities that are associated with DMEPOS suppliers, such as marketing agencies and call centers.[34]

- **Partner with social media companies to prevent the sale of enrollee identification numbers on their platforms.** CMS, in coordination with Federal and State partners, should work with social media companies to prevent the sale of enrollee information on their platforms.

- **Engage Medicare enrollees in the fight against fraud.** CMS should continue to educate enrollees about fraud so they stay vigilant about protecting their identification number. In addition, CMS should explore ways to further engage enrollees in stopping fraud. One option is to develop an enrollee verification

program that would allow CMS to contact enrollees and ask them to verify that they received DMEPOS that they needed, either on a routine basis or for unusual or suspicious claims.

Bolder actions for consideration:

- **Change the way Medicare protects enrollee identification numbers.** More significant changes should be developed to stop enrollee identification numbers from being stolen and misused. CMS should develop new approaches for protecting these numbers. For example, Medicare could integrate ideas and technologies from other industries—such as the credit card industry—into the way it protects identification numbers.

Conclusion

Fraudulent billing for DMEPOS costs taxpayers and the Government millions of dollars each year. Bold action is needed to combat DMEPOS fraud in Medicare and protect the Medicare program and enrollees.

CMS has recently taken a number of steps to strengthen its program integrity tools and increase its oversight of DMEPOS suppliers. For example, CMS is working with its partners through its new Fraud Defense Operations Center to more proactively identify suspect billing and suspend payments. CMS also imposed a 6-month nationwide moratorium on Medicare enrollment of new DMEPOS suppliers so that it could explore additional safeguards to address DMEPOS fraud.

Nonetheless, DMEPOS fraud continues to be a significant concern in Medicare as bad actors develop new schemes to evade oversight. To address this fraud, it is imperative that CMS and others continue to advance fraud-fighting efforts.

To assist in these efforts, this white paper provides a roadmap and offers actions that CMS and others can take to:

- Block fraud at the front door by strengthening Medicare enrollment;
- Catch fake physician orders and claims to stop fueling fraud; and
- Stop the use of stolen enrollee identification numbers to shut down fraud.

These actions would strengthen existing safeguards and address underlying problems that allow fraud to persist. Both are urgently needed to combat DMEPOS fraud, prevent bad actors from diverting money from Medicare and taxpayers, and ensure that Medicare dollars are spent on needed health care for enrollees.

Methodology

This white paper is based on expertise from past OIG investigations, audits, and evaluations. It is also based on structured interviews with CMS staff, CMS contractors, and Medicare Advantage organizations. We also conducted reviews of key documents, relevant regulations, and CMS guidance.

Insights from OIG

We gathered insights from OIG's extensive body of work on DMEPOS, as well as OIG subject matter experts. As a part of this process, we reviewed past OIG investigations, audits, and evaluations related to oversight and billing for DMEPOS. We also interviewed OIG investigators with firsthand experience investigating DMEPOS fraud cases. We discussed the nature of DMEPOS fraud, the vulnerabilities that may have contributed to this fraud, and changes that could prevent this fraud. We also interviewed OIG attorneys, auditors, and evaluators with DMEPOS subject matter expertise to gain insights from their work.

Structured Interviews

We conducted structured interviews with CMS staff, CMS contractors, and Medicare Advantage organizations. This process included interviews with:

- CMS related to enrollment, claims processing, and program oversight, among other functions.[35]
- CMS contractors including a DME Medicare Administrative Contractor, a National Provider Enrollment Contractor, a Unified Program Integrity Contractor, and the Investigations Medicare Drug Integrity Contractor.
- Six selected Medicare Advantage organizations.

Document Review

We reviewed key CMS documents related to Medicare DMEPOS supplier enrollment, billing, and safeguards, among others. These documents included statutes, regulations, and CMS guidance. We also reviewed DMEPOS fraud cases and related documents, such as indictments.

Limitations

This white paper is based on OIG expertise, interview data, and a document review. We did not review Medicare claims data or conduct medical record review as a part of this product.

Standards

We conducted this study in accordance with the *Quality Standards for Inspection and Evaluation* issued in 2020 by the Council of the Inspectors General on Integrity and Efficiency.

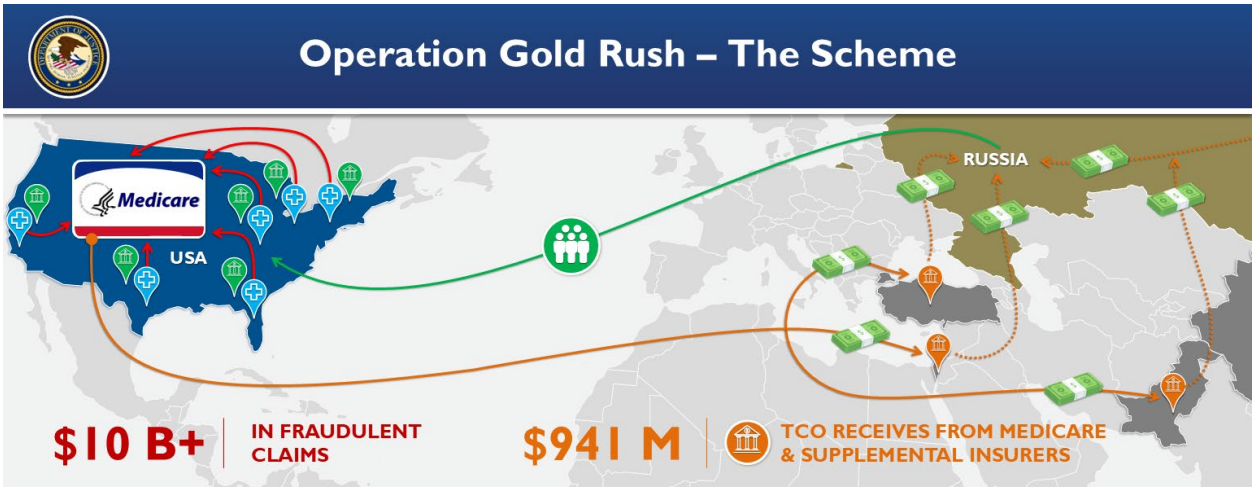
Appendix A

Operation Gold Rush Uncovered an Alleged DMEPOS Fraud Scheme That Billed Medicare for More Than $10 Billion

A transnational criminal organization (TCO)—based outside the United States—is alleged to have orchestrated a complex DMEPOS fraud scheme that billed Medicare for more than $10 billion.

According to the indictment, the organization purchased over 30 DMEPOS suppliers across the country that were already enrolled in Medicare and failed to inform CMS of the changes of ownership. The organization sent individuals from overseas to the United States to act as straw owners for the purchased companies. The straw owners used false documentation to open U.S. bank accounts for the DMEPOS suppliers. Once the bank accounts were established, the criminal organization submitted over $10 billion in fraudulent claims for urinary catheters and other medical equipment, using stolen enrollee identifiers without physician orders or patient medical necessity. The patients never received the DMEPOS items.

However, this high-volume billing was detected by HHS-OIG and CMS, and CMS implemented payment suspensions to stop the vast majority of payments for these billings. Yet, the criminal organization still received $941 million from Medicare and Medicare secondary payers—such as Medigap insurers—and laundered the money to overseas accounts.



Source: Department of Justice, 2025.

Appendix B

CMS Comments and OIG Response

OIG appreciates the partnership with CMS to combat DMEPOS fraud. We support the initial steps that CMS has taken to begin implementing several calls to action outlined in this white paper. As CMS notes, it recently issued a Request for Information seeking public input on several of the issues discussed in this paper, and it has initiated a moratorium on new enrollments for certain DMEPOS suppliers so that it could explore additional safeguards. We look forward to continuing our collaboration with CMS as it takes other actions to prevent DMEPOS fraud and protect both taxpayer dollars and the Medicare program.

Following this page are the official comments from CMS.

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: July 23, 2026

TO: Melicia Seay
Assistant Inspector General for Evaluation and Inspections
Office of Inspector General

FROM: Dr. Mehmet Oz DR
Administrator
Centers for Medicare & Medicaid Services

SUBJECT: Office of Inspector General (OIG) Draft *White Paper: The Nation's Challenge to Combat Durable Medical Equipment Fraud in Medicare* (OEI-02-24-00311)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft white paper.

Medicare Part B covers medically necessary Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) items that are furnished by Medicare enrolled DMEPOS suppliers and that meet other requirements specified in statute and regulation. Suppliers are tasked with submitting the claim and supplying the item. For some items covered under Original Medicare, CMS requires prior authorization and/or a face-to-face encounter with a health care provider and a written order prior to delivery. DMEPOS has been a frequent target of fraud and has a high improper payment rate. However, CMS is taking decisive steps to prevent fraudulent Medicare billing by DMEPOS companies.

In March 2025, CMS launched the Fraud Defense Operations Center (FDOC), better known as the Medicare War Room. In its first year, the Medicare War Room has become one of the most powerful weapons in the fight against fraud, waste, and abuse in Medicare history, stopping billions of dollars from reaching bad actors. The Medicare War Room is a cross-functional strike force uniting elite data analysts, investigators, health policy experts, legal advisors, and law enforcement under one roof with a single mission: stop fraud before taxpayers lose a single dollar. By harnessing rigorous, data-driven intelligence, the Medicare War Room detects threats in real time, coordinates rapid intervention, and shuts down inappropriate billing before it ever hits Medicare's books. In its first year, the Medicare War Room suspended over $2.1 billion in potentially fraudulent payments including over $1.9 billion for suspect DMEPOS billing.[1] This is directly responsive to OIG's calls to action to enhance the use of payment suspensions and to harness new technologies and analytic tools to better detect and stop payments for fraudulent DMEPOS claims.

[1] This data includes March 31, 2025-March 31, 2026, and are therefore subject to change.

In fact, due to the bold actions this administration has taken to crush fraud, CMS delivered unprecedented results in Fiscal Year (FY) 2025, protecting taxpayer dollars and holding bad actors accountable like never before. Total Medicare program integrity savings surged 59 percent, from $26.3 billion in FY 2024 to $41.9 billion in FY 2025. CMS prioritized "stop and caught" activities over "pay and chase" methods like recoupment. Cost avoidance activities, such as revocations or automated claim denials, accounted for 68 percent of all FY 2025 savings.

In February 2026, CMS announced a six-month moratorium on new Medicare enrollment for certain DMEPOS suppliers. A moratorium is a temporary suspension or halt on the enrollment of new providers or suppliers in specific categories or geographic areas. CMS implements moratoria as a program integrity measure by stopping enrollment of new providers in areas or categories where there is a significant potential for fraud, waste, and abuse. This moratorium applies to all applications for initial enrollment and changes in majority ownership for medical supply companies. The moratorium allows CMS to explore additional safeguards to further mitigate longstanding instances of fraud, waste, and abuse perpetrated by certain DMEPOS companies. This directly responds to OIG's call to action to increase oversight of newly enrolled DMEPOS suppliers and suppliers with recent ownership changes.

Also in February 2026, CMS issued a Request for Information (RFI) to collect stakeholder input on ways to better prevent, identify, and address fraud, waste, and abuse that could be considered as part of an upcoming Comprehensive Regulations to Uncover Suspicious Healthcare (CRUSH) Rule. The comment period closed on March 30th and CMS is reviewing over 500 comments received. Topics within the RFI include reducing risks from non-participating DMEPOS suppliers in Medicare Advantage, reducing the claim filing timeline for high-risk items and services including DMEPOS, unsolicited outreach to Medicare beneficiaries, and the surety bond requirement for DMEPOS suppliers. These RFI topics directly respond to OIG's calls to action to require Medicare Advantage-only DMEPOS suppliers to enroll in Medicare, reassess the DMEPOS surety bond requirement, and expand the prohibition on unsolicited outreach to Medicare enrollees to additional forms of contact and associated third-party entities.

In March 2026, CMS released a publicly available list of revoked Medicare enrollments. This dataset contains a point-in-time list of providers and suppliers whose Medicare enrollment has been revoked and who remain under an active re-enrollment bar. It is designed to help users identify revoked Medicare enrollments that were still subject to a bar on re-entering the program. This additional transparency allows patients and payers, including private insurers, to understand which providers have been subject to such administrative enforcement action by the government.[2] This transparency measure complements OIG's broader call to action to strengthen safeguards against bad actors gaining access to Medicare-enrolled DMEPOS suppliers.

In addition to these recent efforts, CMS also has several ongoing initiatives aimed at addressing fraud, waste, and abuse. The DMEPOS Competitive Bidding Program has been an essential tool to help Medicare set market-based payment rates for DMEPOS items, save money for beneficiaries and taxpayers, and limit fraud and abuse in the Medicare Program. The DMEPOS Competitive Bidding Program has saved billions of dollars since its implementation while safeguarding access to quality items and services. Under the DMEPOS Competitive Bidding

[2] Data is available at: https://data.cms.gov/search?keywords=Revoked+Medicare+Providers+and+Suppliers&sort=Relevancy

Program, DMEPOS suppliers compete to become Medicare contract suppliers by submitting bids to furnish certain items in competitive bidding areas. The statute requires that single payment amounts replace the current Medicare DMEPOS fee schedule payment amounts for competitively bid DMEPOS items and services furnished in competitive bidding areas of the country. The single payment amounts are determined by using bids submitted by DMEPOS suppliers.

The DMEPOS Competitive Bidding Program is currently in a temporary gap period while CMS is making some important changes to the program. The product categories for the next round include Class II continuous glucose monitors (CGMs) and insulin pumps, urological supplies, ostomy supplies, hydrophilic catheters, off-the-shelf (OTS) back braces, OTS knee braces, and OTS upper extremity braces. The next round of competitive bidding is expected to take effect January 1, 2028.[3]

As part of CMS's strategy to prevent improper payments and protect the Medicare Trust funds, Medicare contractors and internal CMS staff utilize advanced analytics, including the use of artificial intelligence (AI), to identify billing outliers and anomalous claim patterns. Once identified, Medicare contractors conduct medical review to further assess suspicious behavior. Medical review involves the collection and clinical review of medical records and related information to ensure that payment is made only for services that meet all Medicare coverage, coding, billing and medical necessity requirements. When errors are identified, improper payments are recovered and education is provided to ensure future compliance. The Medicare contractors have completed several projects specifically targeting vulnerabilities such as new suppliers, surgical dressings, continuous glucose monitors and supplies, and wound care. These projects are separate from the standard medical review workload that includes review, recoupment, and education. These activities are directly responsive to OIG's calls to action to harness new technologies and analytic tools to detect and stop payments for fraudulent DMEPOS claims and to expand medical reviews to prevent fraud, including through pre-payment review of new suppliers.

CMS has taken several steps to stop the theft and misuse of stolen Medicare Beneficiary Identifiers (MBIs) including enhancing monitoring of its lookup tools and hosting IDea Challenges, a series of in-person, solution-oriented events designed to generate actionable ideas to enhance MBI security. CMS will continue this work and explore new approaches, including those that work in other industries, to help address misused MBIs. This work is directly responsive to OIG's call to action to better protect enrollee lookup tools and, more broadly, to its bolder recommendation that Medicare change how it protects enrollee identification numbers by adapting approaches used in other industries.

CMS also continues to educate health care providers and suppliers on the proper billing of Medicare items and services, as well as ways to prevent, detect and report Medicare fraud and abuse. The Medicare Learning Network (MLN) provides education and support for Medicare providers and suppliers[4]. The MLN publishes weekly newsletters that highlight new and revised Medicare policies, upcoming educational events and deadlines, links to new MLN products and resources, and reminders about billing and coding updates. The MLN has a variety of

[3] Information on the next round of DMEPOS Competitive Bidding is available at: https://dmeposcompetitivebid.cms.gov/node/636.
[4] The Medicare Learning Network (MLN) may be accessed at: https://www.cms.gov/training-education/medicare-learning-networkr-mln/resources-training.

publications related to DMPEOS billing, as well as print materials and a web-based training on preventing, detecting, and reporting Medicare fraud and abuse.[5] Additionally, CMS maintains a webpage dedicated to crushing fraud, waste, and abuse which includes a spotlight feature on DMEPOS fraud.[6]

Additionally, CMS employs a wide range of strategies to educate Medicare beneficiaries about fraud and how they can protect themselves. For example, CMS maintains webpages which include information on reporting Medicare fraud and abuse, including recent scams.[7] CMS uses social media, email, and publications such as the Medicare & You handbook to educate beneficiaries.[8] Through our Annual Medicare Fraud National Outreach and Education Campaign, we deliver messages on getting wise to Medicare fraud and provide the public with the information they need to detect, prevent, and report Medicare fraud. CMS encourages beneficiaries to regularly review their Medicare Summary Notices, which detail services billed to Medicare on their behalf. CMS partners with the Senior Medicare Patrol which empowers and assists Medicare beneficiaries, their families, and caregivers to prevent, detect, and report health care fraud, errors, and abuse through outreach, counseling, and education. These actions highlight CMS's ongoing effort to address OIG's call to action to engage Medicare enrollees in the fight against fraud.

Taken together, the initiatives described above directly respond to the majority of OIG's calls to action across all three areas addressed in the white paper — DMEPOS supplier enrollment, physician orders, and enrollee identification numbers. CMS appreciates OIG's suggestions in the smaller number of calls to action that CMS has yet to address. Many of these suggestions are under consideration and will be addressed in CMS's upcoming CRUSH regulation which is expected to be published in proposed form later this year.

As demonstrated above, CMS continues to build on its broad strategy to combat fraud, waste, and abuse through data-driven prevention and real-time enforcement. CMS is making unprecedented progress in its fight to crush fraud and appreciates OIG's work and partnership in this area.

[5] MLN Booklet. Medicare Fraud & Abuse: Prevent, Detect, Report is available at: https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/fraud-abuse-mln4649244.pdf; MLN Web-based Training Course. Medicare Fraud & Abuse: Prevent, Detect, Report is available at: https://www.cms.gov/Outreach-and-Education/MLN/WBT/MedicareFraudandAbuse/FraudandAbuse/story.html.
[6] The CMS fraud webpage may be accessed at: https://www.cms.gov/fraud. The feature on DMEPOS is available at: https://www.cms.gov/files/document/hot-spot-dmepos-suppliers.pdf.
[7] Please see: https://www.medicare.gov/basics/reporting-medicare-fraud-and-abuse.
[8] The Medicare & You handbook is available at: https://www.medicare.gov/medicare-and-you.

Appendix C

Prior Related OIG Work

Report Title	Report Number	Year Issued
Medicare Improperly Paid Suppliers $22.7 Million Over 7 Years for Durable Medical Equipment, Prosthetics, Orthotics, and Supplies Provided to Enrollees During Inpatient Stays	OAS-24-09-005	2025
Medicare Remains Vulnerable to Fraud, Waste, and Abuse Related to Off-the-Shelf Orthotic Braces, Which May Result in Improper Payments and Impact the Health of Enrollees	A-09-21-03019	2024
Medicare Improperly Paid Durable Medical Equipment Suppliers an Estimated $8 Million of the $40 Million Paid for Power Mobility Device Repairs	A-09-20-03016	2022
Medicare Improperly Paid Suppliers an Estimated $117 Million Over 4 Years for Durable Medical Equipment, Prosthetics, Orthotics, and Supplies Provided to Hospice Beneficiaries	A-09-20-03026	2021
CMS's Encounter Data Lack Essential Information That Medicare Advantage Organizations Have the Ability to Collect	OEI-03-19-00430	2020
Incomplete and Inaccurate Licensure Data Allowed Some Suppliers in Round 2 of the Durable Medical Equipment Competitive Bidding Program That Did Not Have Required Licenses	A-05-13-00047	2016
Enhanced Enrollment Screening of Medicare Providers: Early Implementation Results	OEI-03-13-00050	2016
Escalating Medicare Billing for Ventilators Raises Concerns	OEI-12-15-00370	2016
Medicare Paid Suppliers for Power Mobility Device Claims That Did Not Meet Federal Requirements for Physicians' Face-to-Face Examinations of Beneficiaries	A-09-12-02068	2015
Surety Bonds Remain an Underutilized Tool To Protect Medicare From Supplier Overpayments	OEI-03-11-00350	2013
Inappropriate and Questionable Medicare Billing for Diabetes Test Strips	OEI-04-11-00330	2013
CMS Response to Breaches and Medical Identity Theft	OEI-02-10-00040	2012
CMS Has Not Promulgated Regulations To Establish Payment Requirements for Prosthetics and Custom-Fabricated Orthotics	OEI-07-10-00410	2012
Claim Modifier Did Not Prevent Medicare From Paying Millions in Unallowable Claims for Selected Durable Medical Equipment	A-04-10-04004	2012
Program Integrity Problems With Newly Enrolled Medicare Equipment Suppliers	OEI-06-09-00230	2011
Questionable Billing by Suppliers of Lower Limb Prostheses	OEI-02-10-00170	2011
Most Power Wheelchairs in the Medicare Program Did Not Meet Medical Necessity Guidelines	OEI-04-09-00260	2011

* For forthcoming OIG work, see the OIG work plans for medical equipment and supplies.

Endnotes

[1] CMS also uses the term "Fraud War Room" to refer to its new Fraud Defense Operations Center (FDOC). Through the FDOC, CMS works with its partners to identify suspect billing—e.g., billing with fake physician orders—and suspend payments. The FDOC includes a team of experts in various fields and utilizes advanced data analytics. CMS, *Fraud Defense Operations Center Fast Facts*, January 2026. Accessed at https://www.cms.gov/files/document/fdoc-fact-sheet-updated.pdf on Mar. 12, 2026.

[2] Department of Justice (DOJ), "11 Defendants Indicted in Multi-Billion Health Care Fraud Scheme, the Largest Case by Loss Amount Ever Charged by the Department Of Justice" (press release, June 30, 2025). Accessed at https://www.justice.gov/usao-edny/pr/11-defendants-indicted-multi-billion-health-care-fraud-scheme-largest-case-loss-amount on Mar. 19, 2026.

[3] DOJ, "South Carolina U.S. Attorney Announces Operation Dismantling One of the Largest Medicare Fraud Schemes in History" (press release, Apr. 10, 2019). Accessed at https://www.justice.gov/usao-sc/pr/south-carolina-us-attorney-announces-operation-dismantling-one-largest-medicare-fraud on June 18, 2026.

[4] The moratorium also halts enrollments that result from changes of majority ownership. See 91 Fed. Reg. 9855 (Feb. 27, 2026).

[5] DOJ, "11 Defendants Indicted in Multi-Billion Health Care Fraud Scheme, the Largest Case by Loss Amount Ever Charged by the Department of Justice" (press release, June 30, 2025). Accessed at https://www.justice.gov/usao-edny/pr/11-defendants-indicted-multi-billion-health-care-fraud-scheme-largest-case-loss-amount on Mar. 19, 2026.

[6] See 42 CFR § 424.57. This requirement applies only to suppliers billing Original Medicare, also known as Medicare fee-for-service. It does not apply to suppliers billing only Medicare Advantage.

[7] DOJ, "Florida Man Pleads Guilty to Conspiring to Defraud Medicare of $39.5 Million" (press release, Aug. 15, 2024). Accessed at https://www.justice.gov/usao-nh/pr/florida-man-pleads-guilty-conspiring-defraud-medicare-395-million on June 16, 2026.

[8] For more information about enrollment requirements and the enrollment process, see 42 CFR § 424.57 and CMS, *Medicare Program Integrity Manual, Chapter 10 – Medicare Enrollment,* Aug. 13, 2025. Accessed at https://www.cms.gov/regulations-and-guidance/guidance/manuals/downloads/pim83c10.pdf on Feb. 24, 2026.

[9] 42 CFR §§ 424.518(c)(1)(ii), (c)(2)(i), and (b)(2)(ii) (requiring on-site visits for newly enrolling DMEPOS suppliers) and 42 CFR § 424.57(c). DMEPOS supplier on-site inspections include interviews and validate signage, hours, inventory, equipment maintenance, record storage, and complaint policies. This includes verifying that the DMEPOS supplier has a business phone number that is listed in a directory and is not a cell phone number.

[10] Certain DMEPOS suppliers, such as occupational therapists, orthotists, and physicians (among others) are exempt from surety bond requirements. 42 CFR § 424.57(d)(15). For more information see Novitas Solutions, "Accreditation and surety bond exemptions," updated Jan. 20, 2026. Accessed at https://www.novitas-solutions.com/webcenter/portal/DMEPOS/pagebyid?contentId=00277116 on Apr. 28, 2026.

[11] OIG, *Surety Bonds Remain an Underutilized Tool To Protect Medicare From Supplier Overpayments* (OEI-03-11-00350), Mar. 21, 2013. Accessed at https://oig.hhs.gov/reports/all/2013/surety-bonds-remain-an-underutilized-tool-to-protect-medicare-from-supplier-overpayments/ on Feb. 11, 2026.

[12] At the Federal level, the Department of Treasury collects some—but not all—ownership data. For more information about data maintained by the Department of Treasury, see GAO, *Fraud in Federal Programs: FinCEN Should Take Steps to Improve the Ability of Inspectors General to Determine Beneficial Owners of Companies*, Apr. 8, 2025. Accessed at https://files.gao.gov/reports/GAO-25-107143/index.html?_gl=1*1qkv3b9*_ga*MTEzNTk0ODYxMi4xNzYyOTgxMzE4*_ga_V393SNS3SR*czE3NzczMDkzNTckbzckZzEkdDE3NzczMDk2MTMkajU1JGwwJGgw on Apr. 28, 2026.

[13] For instance, CMS made changes in the steps suppliers need to take following changes of majority ownership. 90 Fed. Reg. 55342, 55618-19 (Dec. 2, 2025) (effective Jan. 1, 2026). CMS now requires DMEPOS suppliers to re-enroll in Medicare if they have a change in majority ownership within 3 years of enrolling or changing majority ownership. 42 CFR § 424.551.

[14] CMS should incorporate exceptions to this requirement, as necessary.

[15] For more information about billing by new suppliers, see OIG, *Medicare Remains Vulnerable to Fraud, Waste, and Abuse Related to Off-the-Shelf Orthotic Braces, Which May Result in Improper Payments and Impact the Health of Enrollees* (A-09-21-03019), May 24, 2024. Accessed at https://oig.hhs.gov/reports/all/2024/medicare-remains-vulnerable-to-fraud-waste-and-abuse-related-to-off-the-shelf-orthotic-braces-which-may-result-in-improper-payments-and-impact-the-health-of-enrollees/ on June 17, 2026.

[16] CMS implemented a similar approach for hospices. It implemented a provisional period of enhanced oversight in six States for certain hospices, including those that newly enrolled in Medicare and those that changed ownership. For more information see CMS, "Period of Enhanced Oversight for New Hospices in Arizona, California, Nevada, Texas, Georgia & Ohio," February 2026. Accessed at https://www.cms.gov/files/document/mln7867599-period-enhanced-oversight-new-hospices-arizona-california-nevada-texas-georgia-ohio.pdf on June 16, 2026.

[17] See OIG's work plan, *CMS's Use of Surety Bonds To Protect Medicare Part B From Overpayments to Durable Medical Equipment Suppliers* (OEI-03-25-00080), Feb. 17, 2025. Accessed at https://oig.hhs.gov/reports/work-plan/browse-work-plan-projects/cmss-use-of-surety-bonds-to-protect-medicare-part-b-from-overpayments-to-durable-medical-equipment-suppliers/ on Mar. 23, 2026. For prior OIG work on surety bonds, see OIG, *Surety Bonds Remain an Underutilized Tool To Protect Medicare From Supplier Overpayments* (OEI-03-11-00350), Mar. 21, 2013. Accessed at https://oig.hhs.gov/reports/all/2013/surety-bonds-remain-an-underutilized-tool-to-protect-medicare-from-supplier-overpayments/ on Feb. 11, 2026.

[18] Of note, CMS recently published a Request for Information seeking input on changes it could make to more effectively crush fraud. As a part of this request, CMS is seeking input on whether Medicare Advantage organizations would prefer that all DMEPOS suppliers be enrolled, ensuring that they meet minimum supplier standards. See 91 Fed. Reg. 9803, 9806 (Feb. 27, 2026).

[19] OIG, *Medicare Advantage Organizations and CMS Can Do More To Prevent Durable Medical Equipment Fraud in Medicare Advantage* (OEI-02-24-00310), forthcoming.

[20] All DMEPOS items require a written order from a treating practitioner as a condition of payment. 42 CFR §§ 410.38(c)(4) and (d). In this white paper, "physician" refers to any practitioner who meets the

definition of a treating practitioner, including a physician, physician assistant, nurse practitioner, or clinical nurse specialist. 42 CFR §410.38(c)(2).

[21] DOJ, "Michigan Doctor Sentenced to Four Years for $6.3M Medicare Fraud Scheme" (press release, June 26, 2025). Accessed at https://www.justice.gov/opa/pr/michigan-doctor-sentenced-four-years-63m-medicare-fraud-scheme on Mar. 3, 2026.

[22] DOJ, "Chula Vista Man Pleads Guilty in $51 Million Medicare Fraud Scheme" (press release, May 27, 2025). Accessed at https://www.justice.gov/usao-sdca/pr/chula-vista-man-pleads-guilty-51-million-medicare-fraud-scheme on Mar. 19, 2026.

[23] These reviews are called "Targeted Probe and Educate." They focus on correcting billing errors. See CMS, "Targeted Probe and Educate." Accessed at https://www.cms.gov/data-research/monitoring-programs/medicare-fee-service-compliance-programs/medical-review-and-education/targeted-probe-and-educate-tpe on Mar. 3, 2026.

[24] CMS can suspend payments when it has creditable allegations of fraud. 42 CFR § 405.371(a)(2).

[25] For example, DOJ estimates that DMEPOS suppliers involved in Operation Gold Rush received about $900 million from Medigap and other secondary payors. DOJ, "11 Defendants Indicted in Multi-Billion Health Care Fraud Scheme, the Largest Case by Loss Amount Ever Charged by the Department of Justice" (press release, June 30, 2025). Accessed at https://www.justice.gov/usao-edny/pr/11-defendants-indicted-multi-billion-health-care-fraud-scheme-largest-case-loss-amount on Mar. 19, 2026.

[26] OIG, *CMS's Encounter Data Lack Essential Information That Medicare Advantage Organizations Have the Ability To Collect* (OEI-03-19-00430), August 2020. Accessed at https://oig.hhs.gov/documents/evaluation/2805/OEI-03-19-00430-Complete%20Report.pdf on July 9, 2026.

[27] For example, certain DMEPOS suppliers that are compliant with Medicare requirements are now exempt from prior authorization. This allows CMS to focus its efforts on suppliers that pose a higher risk. See 90 Fed. Reg. at 55603 (adding paragraphs (c)(1)(ii)(A) and (B) to 42 CFR § 414.234).

[28] This could be similar to how CMS has used enhanced technology assistance for its Risk Adjustment Data Validation audits. See CMS, "CMS Rolls Out Aggressive Strategy to Enhance and Accelerate Medicare Advantage Audits" (press release, May 21, 2025). Accessed at https://www.cms.gov/newsroom/press-releases/cms-rolls-out-aggressive-strategy-enhance-and-accelerate-medicare-advantage-audits on Mar. 3, 2026.

[29] OIG, *CMS's Encounter Data Lack Essential Information That Medicare Advantage Organizations Have the Ability To Collect* (OEI-03-19-00430), August 2020. Accessed at https://oig.hhs.gov/documents/evaluation/2805/OEI-03-19-00430-Complete%20Report.pdf on July 9, 2026.

[30] DOJ, "Florida Man Sentenced in Multi-Million-Dollar Medicare Fraud Scheme" (press release, Feb. 17, 2022). Accessed at https://www.justice.gov/usao-ma/pr/florida-man-sentenced-multi-million-dollar-medicare-fraud-scheme on Mar. 19, 2026.

[31] These tools are hosted by the Medicare Administrative Contractors and are called the Medicare Beneficiary Identifier lookup tools. CMS restricts access to these tools to registered users and requires password-protected authentication. CMS also emphasizes that providers and suppliers should use these tools only when patients do not provide their identification number.

[32] For example, CMS increased monitoring of its enrollee identification number lookup tools. It also convened meetings with experts to develop ideas to improve the security of enrollee identification numbers. For more information, see CMS, *MLN Connects Newsletter*, February 2026. Accessed at https://www.cms.gov/training-education/medicare-learning-network/newsletter/mln-connects-newsletter-february-26-2026#_Toc222983696 on Mar. 11, 2026. See also, CMS, "2025 CMS IDea Challenge: Strategies for Securing Member IDs: Frequently Asked Questions (FAQs)," September 2025. Accessed at https://www.cms.gov/files/document/crushing-fraud-idea-challenge-faqs.pdf on Mar. 11, 2026.

[33] Suppliers with patterns of unsolicited contact can be excluded from Medicare and other federally funded health care programs. Social Security Act, § 1834(a)(17)(c), § 42 U.S.C. 1395m(a)(17)(c).

[34] Social Security Act, §§ 1834(a)(17)(B) and (C).

[35] CMS responded to the structured interview questions in writing.

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

 OIGatHHS

 HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov