AAHOMECARE
American Association for Homecare

Submitted via: www.regulations.gov

March 30, 2026

Dr. Mehmet C. Oz, M.D.
Administrator
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244

RE: Response to CMS Request for Information (RFI) Related to Comprehensive Regulations to Uncover Suspicious Healthcare (CRUSH)

Dear Administrator Oz,

Introduction

Thank you for the opportunity to submit comments in response to the Request for Information (RFI), Related to Comprehensive Regulations to Uncover Suspicious Healthcare (CRUSH). We appreciate CMS's continued efforts to strengthen program integrity and address fraud and abuse across the healthcare system.

The American Association for Homecare (AAHomecare) is the national association representing durable medical equipment, prosthetics, orthotics and supplies (DMEPOS) suppliers, manufacturers, and other stakeholders in the homecare community. Our members are proud to be part of the continuum of care that assures beneficiaries and other patients receive cost effective, safe, and reliable home care products and services.

AAHomecare Position on Fraud, Waste, and Abuse

As the leading voice for the DMEPOS community, we are committed to being a good steward of the Medicare program and fully support the Agency's ongoing efforts to eliminate fraudulent activity within the marketplace. We recognize that fraud not only drains critical resources but also creates an unfair "black eye" for the thousands of legitimate, law-abiding suppliers who serve the most vulnerable patient populations. Fraudulent activity is dangerous to patients who may experience delays in life-saving services. AAHomecare is engaged with the Administration and CMS in combating fraud and abuse within the DMEPOS industry and has had several opportunities to discuss ways the Association can work with CMS on improving existing programs and developing pilot programs.

The services our members provide are essential in keeping beneficiaries safe in their homes while they are being treated. Most patients prefer to be in their home rather than being treated in an inpatient setting. Every day, our members are connecting with patients to ensure they are safely using their DMEPOS products to allow them to live healthily and comfortably. **To ensure any fraud fighting efforts are successful without inadvertently harming patients and the legitimate DMEPOS supplier community, we urge CMS to adopt**

a more nuanced and strategic approach that targets at-risk and bad actors while minimizing the administrative burden on ethical suppliers.

AAHomecare Recommendations

AAHomecare's comments offer a broad strategic overview of our recommended regulatory initiative to effectively address fraudulent activity.

Strengthen Provider Enrollment Requirements for New DMEPOS Suppliers

To prevent fraudulent entities from cycling through the Medicare system, AAHomecare recommends implementing a robust identity verification and authentication process to ensure bad actors cannot enter or re-enter under new company names. This could be an internal CMS verification process such as reviewing a cross-section of internal government data that would identify fraudulent players from the broader healthcare sector and other industries, creating a check for new companies entering and fraudulent entities from reentering.

The enrollment process for all new companies should be subject to a multi-layered verification process to ensure they are entering the Medicare market in good faith.

However, CMS should also consider instituting a system that validates DMEPOS companies to ensure that the administrative scrutiny is applied only towards unknown or high-risk entities rather than suppliers with a proven compliant history. A broad, across-the-board increase in provider enrollment requirements would impose a significant administrative burden on all suppliers, with limited benefits to preventing fraudulent entities from entry. Any such efforts should be targeted and risk-based to be effective.

Improve Quality of Site Visits

There is a critical need to improve the quality of site visits. Although site inspectors are employed to ensure supplier locations are meeting the Medicare supplier standards, the industry has seen over the last several years that many of the site inspectors are not experienced or knowledgeable, and some interactions fall short of professional standards. DMEPOS supplier standards are in place to ensure the legitimacy, quality, and accountability of supplier businesses participating in Medicare. Site inspections are a critical component of CMS's oversight process. Site visits carry significant weight for suppliers, an unfavorable finding can result in revocation of their supplier number, which prevents the business from billing and jeopardizes their ability to continue to service patients. This is especially heightened for suppliers operating with small margins, even a short-term disruption can have a disproportionate consequence on their business viability.

Over the last several years, we have heard from our supplier members about their experiences with unknowledgeable and unengaged site inspectors who report inaccurate findings, resulting in supplier locations being revoked. The steep penalties of site visits warrant a requirement for inspectors to be well-informed and committed to providing professional services. AAHomecare recommends that CMS review the number of deactivations and revocations due to unfavorable site inspections that are subsequently reinstated to identify systemic issues surrounding site inspections. AAHomecare also recommends that CMS ensure that individuals employed to conduct site inspections are qualified and properly trained. The quality of site inspections is a critical component of program integrity, and it is only as good as the inspectors with whom CMS contracts.

Improve Cross-Program Enforcement

If a company's Medicare Fee-for-Service (FFS) status is revoked, that revocation should be applied across all government healthcare programs, including Medicare Advantage (MA) and state Medicaid programs but only after the revocation has reached its final stage and all appeal rights have been exhausted. Establishing cross-program revocation is essential because fraudulent entities often exploit the current lack of communication and consistency between the programs. The RFI explicitly notes instances where suppliers revoked under Medicare FFS remained active in MA plans, highlighting a critical gap in program integrity that allows bad actors to continue receiving government funds despite being disqualified from one part of the program. Applying revocations uniformly across all government healthcare programs ensures that once a company is deemed a bad actor, they are completely removed from the ecosystem, preventing them from simply shifting their fraudulent activity to a different payer.

By creating a unified "red flag" system, the Agency can ensure that a revocation based on fraudulent activity is final and comprehensive, effectively barring bad actors from the entire government healthcare landscape.

CMS must ensure that revocations and deactivations are warranted. As previously indicated, there are many examples where the supplier number is revoked or deactivated in error. Similarly, when a supplier appeals a revocation or deactivation, the revocation or deactivation should not be flagged to other programs until a final determination is made. An appeal signifies that the supplier is actively working to fix the issue in good faith, which is an action that is inconsistent with fraudulent players.

In a similar effect, when a supplier number is reinstated, the update must be instantly communicated consistently across all government healthcare programs.

Monitor Electronic Funds Transfer (EFT) Activity of New Suppliers

CMS should monitor EFT activity of new suppliers. Anytime an EFT is set up or changed, CMS should verify whether there has been a corresponding change in ownership or other activity that warrants a review. When there are large deposits or transfers, the transactions should be monitored, like the banking industry monitors large deposits or transfers. By monitoring EFTs of DMEPOS suppliers, CMS will be able to detect potentially fraudulent activity early.

Fraud prevention must be multilayered. While increased provider enrollment scrutiny can improve the prevention of fraudulent entities from entering Medicare, experience has shown that bad actors are adaptable and will find new ways to enter. Ongoing monitoring, even after their enrollment is approved will fortify CMS's fraud prevention efforts. It is important that CMS distinguish legitimate suppliers so that any additional scrutiny is warranted and does not impose overly burdensome requirements on the entire industry.

Mandate Targeted Probe and Educate (TPE) on New Suppliers

All new supplier locations should be placed in a TPE audit to ensure they are compliant from the start. TPE audits are designed to be educational, and requiring new supplier locations to go through the TPE process will be an opportunity to detect whether the supplier is knowledgeable about the coverage and billing criteria for the product categories they provide. And if a new supplier cannot pass a TPE after three rounds of education and correction, CMS should consider stronger action. Historically, CMS required newly enrolled home health agencies to undergo 100% prepay reviews until it was determined they were legitimate and understood all of CMS's requirements.

Because TPE has a structured review process, it is still possible for a bad actor to participate and conduct faithfully initially and later engage in fraudulent billing activity. Therefore, we recommend that even after the new supplier passes the initial TPE, if aberrant billing is detected, that should indicate the need for the new supplier to be re-reviewed.

Promote Use of Electronic Orders (e-Orders)

CMS should encourage the use of e-orders as it would improve integration between DMEPOS orders and patient medical records, communication between suppliers and providers, and will create a digital audit trail that can be accessed by auditing contractors, making it easier to identify issues when no order exists. As the healthcare system continues towards digitization,[1] DMEPOS orders remain comparatively a few technological steps behind, leaving the industry more vulnerable to fraud and abuse. Establishing a fully digital trail today will strengthen transparency and prepare the industry for the integration of any advanced technologies in the future.

Such infrastructure will further promote CMS's current efforts in stopping fraud early.

Leverage Technology to Review Claims in Real Time

Adoption of technology must be part of the solution in fighting fraud and abuse. Technology available today can enable CMS to review claims as they are submitted. AAHomecare has already engaged CMS to explore a proof of concept where automated claims reviews can pair a written order to the claim and if no order exists, can be flagged for additional review. Such automated review of claims may help detect fraud much earlier than what is being caught today, which will significantly improve efficiency. This type of technology should be adopted by all government health plans including state Medicaid programs, MCOs, and MA plans.

As mentioned above, for this to be a viable option in the future, all orders would need to be electronic and be housed in an e-order repository or data bank, which would allow DME MACs access to review orders as needed.

Create CMS Tech Liaison

Currently, when a DMEPOS technology company that conducts billing or ordering notices aberrant behavior, there is no mechanism in place for the platforms to notify CMS. Nor is there any requirement for them to take any action. With more suppliers opting to digitize their orders, the platforms have a front row seat on various company activities. Engaging with the technology platforms is an opportunity for CMS to be potentially notified earlier in the process and collaborate on fraud-fighting efforts.

Due to the importance of the collaboration, a specific liaison position should be created at CMS to coordinate with technology platforms. The liaison should be knowledgeable and should not be a front-line customer service representative. The role should be filled by an individual or team that is fluent in the DMEPOS industry's requirements.

[1] See e.g., CMS Final Rule, "Administrative Simplification; Adoption of Standards for Health Care Claims Attachments Transactions and Electronic Signatures, CMS-0053-F.

Improve Medicare Advantage (MA) Oversight

The lack of consistency among the hundreds of MA plans has created confusion within the industry and undermines efforts to combat fraud due to the lack of clarity. MA plans should be required to follow all Medicare requirements, including operational, coverage, and payment policies.

MA plans often impose requirements that go beyond traditional Medicare requirements, resulting in inconsistencies across the programs. These can include differing documentation requirements, prior authorization procedures, or coverage policies for the same DMEPOS items. For suppliers and patients, these variations create confusion, increase administrative burden, and can delay or limit access to necessary care. When MA plans follow uniform Medicare rules, CMS and MA plans can more easily detect aberrant billing patterns, ensure consistent enforcement actions, and prevent bad actors from exploiting differences across payers to avoid oversight.

To improve consistency and reduce unnecessary complexity, MA plans should align their requirements with standard Medicare requirements. Consistency also helps CMS maintain program integrity, as it simplifies monitoring and ensures all patients receive coverage according to the same baseline standards.

Expanding Prior Authorization (PA)

There are currently several DMEPOS product categories/HCPCS codes that require PA, and we have seen remarkable success with PA in reducing improper payments. We believe there are opportunities to expand the program to other product categories. PA requires suppliers to submit medical records and orders for review before services are rendered.

The upfront review can streamline the service for patients and suppliers; however, it is important for CMS to consider which DMEPOS product categories are appropriate to be added and be sensitive to the timeframe for the authorizations to be completed. For identified high-risk items that are suited for review, PA can fortify CMS's program integrity efforts.

In addition, PA has been widely supported by suppliers as it provides assurance that their services are approved by CMS in advance, and it also reduces potential post-payment audits. Expanding PA for appropriate DMEPOS items can serve as an initiative-taking measure to prevent fraud and abuse before services are delivered.

DMEPOS Supplier Surety Bond

In the RFI, CMS discusses the option to increase the amount of a surety bond of $50,000 per location to deter fraudulent actors from participating in Medicare. However, such a measure will not be perceived as a barrier to fraudulent actors and instead would disproportionately impact legitimate suppliers. Fraud prevention should be focused on initial enrollment and ongoing oversight.

Improve Transparency on Real Fraud Loss

The DMEPOS industry recognizes that the entry of fraudulent companies is a genuine issue that needs to be addressed. The presence of such malicious entities has cast a dark shadow on the industry when thousands of legitimate DMEPOS suppliers demonstrate strong compliance and care for the millions of beneficiaries they serve. In recent years, there has been significant attention on the $2 billion in intermittent catheter fraud. However, less attention has been given to the fact that CMS was able to prevent over 99% of the

fraudulent claims from being paid.[2] The distinction is crucial and warrants emphasis. CMS's ability to prevent Medicare funds from being transferred to these fraudulent entities showcases the Agency's progress in its program integrity efforts. Focusing on CMS's ability to stop 99% of the $2 billion in fraud provides a more complete and truer picture of what transpired.

Timely Filing Limit

CMS is considering shortening the one-year Medicare claims filing deadline for high-risk items (explicitly including DMEPOS) to 90–180 days. AAHomecare strongly recommends that CMS maintain the claims filing deadline for DMEPOS at one year, as it is consistent with all other Medicare healthcare programs. There are several circumstances where suppliers need to hold claims and delay submitting them to Medicare. For example, a supplier may need to delay submitting or resuming rental claims when a prior rental claim has been denied and is in the appeal process. If a shortened timeframe is implemented, then claims will be filed to meet the timely filing requirements and will then need to be appealed. This will result in many more appeals, rather than allowing a supplier to hold on-going rental claims until the initial claim is overturned and paid.

Participation Status is Not a Fraud Tool

CMS identifies non-participating DMEPOS suppliers billing MA plans as a major fraud risk and signals interest in requiring stricter requirements or standards for non-participating suppliers. Non-participating suppliers are still enrolled in Medicare and are accredited. However, participation status is primarily about payment terms. Participating suppliers must accept the Medicare payment rate, while non-participating suppliers decide on a claim-by-claim basis whether to accept the Medicare rate. Participating status has no influence on fraud risk and should not be used as a fraud control mechanism.

Expand Beneficiary Solicitation Prohibition

CMS is evaluating the expansion of the DMEPOS unsolicited telephone contact prohibition to other communication methods, such as email, text, social media, as well as to third-party marketers acting on behalf of DMEPOS suppliers. Today, the non-solicitation prohibition applies exclusively to phone contact only. AAHomecare supports expanding restrictions on unsolicited beneficiary contact by DMEPOS companies including email, text, and social media. This expansion should not, however, impact supplier marketing that is directed at a specific individual provided that it follows current requirements for contacting a beneficiary.

Improve Oversight and Training of 1-800-Medicare

1-800-Medicare should be used as a frontline tool to identify potential fraud and abuse. As 1-800-Medicare agents interact directly with Medicare beneficiaries regarding service issues, they are uniquely positioned to hear of emerging issues firsthand. Strengthening oversight and follow-up on information gathered by 1-800-Medicare personnel would allow for early intervention.

In addition, the industry has heard that the agents are not sufficiently responsive to beneficiaries' issues. Often, we have seen that when a beneficiary contacts 1-800-Medicare over an explanation of benefits (EOB) that shows Medicare paid for something they did not receive, the agent responds that they have heard the same issue from many others. These types of responses continue to perpetuate a sense of distrust in

[2] As cited in U.S. Department of Health and Human Services Office of Inspector General, Medicare Improperly Paid Suppliers for Intermittent Urinary Catheters, A-09-22-03019 (February 2025), page 13.

beneficiaries that is inappropriate. Beneficiaries who take the initiative to report their issues should feel confident that their concerns will be taken seriously and addressed appropriately.

Require Sellers to Notify the Provider Enrollment Contractors Within Five Business Days of Completing a Sale of Their Business

Under current requirements, the seller and buyer are required to report the transaction within 30 days. This timeframe may allow for a vulnerability that can be exploited by fraudulent entities. AAHomecare recommends that CMS require sellers to notify their provider enrollment contractor of the transaction within five business days. This early reporting would allow CMS to monitor billing activity of the location while anticipating a notification from the buyer within the existing timeframe of 30 days. This notification should simply trigger a watch and should not impact business operations.

Recognizing that a purchase of a business requires the buyer to address other issues related to their application, we support maintaining the current reporting timeframe of 30 days for the buyer while holding a shorter timeframe for the seller.

As with all enrollment transactions, there needs to be transparency in sharing timely information with all other government payers and entities.

Improve PECOS

CMS has been working for many years on creating a PECOS 2.0 with enhanced features to allow suppliers and providers to electronically notify CMS of changes, additions, licensure updates, etc. in real time. However, it is the industry's understanding that PECOS 2.0 has been discontinued at this time.

AAHomecare strongly recommends that CMS invest in PECOS to ensure that ALL transactions, updates, deletions, and changes can be accommodated electronically. CMS must get to the point where there are no paper submissions of enrollment forms. Whether it is a new enrollment, termination, or update.

Often DMEPOS suppliers are forced to submit paper updates to the 855S because the current PECOS system only handles one update at a time and if the record is locked for the change to be processed, any additional changes must be completed on paper to ensure suppliers meet the required time frames for submission.

Require Providers to Report Lead Generation Companies

Although there is no reliable way to measure the prevalence of lead generation companies within the DMEPOS sector, their use is well known, and some have been associated with program integrity concerns. As part of the enrollment process, CMS should require suppliers to disclose lead generation companies that they are contracting with, similar to the way suppliers report third party billing companies. In addition to improved transparency, when an issue arises with one lead generation company, CMS will have the ability to review other DMEPOS companies that have engaged with the same company.

Mandate Healthcare Fraud Prevention Partnership (HFPP) for All Government Healthcare Insurers

HFPP is a CMS-led voluntary public–private partnership to combat healthcare fraud, waste, and abuse. HFPP brings together public and private insurers, anti-fraud associations, federal agencies, and others to share insights and data to prevent fraud across the healthcare system. A program like HFPP is essential because fraudulent entities often shift between healthcare programs and services, and by fostering

collaboration, all stakeholders would be able to proactively identify and prevent emerging threats before they escalate.

Improve Oversight of Audit Contractors

We have observed inconsistencies and challenges with audit contractors for all government health plans, including Medicare FFS, Medicaid FFS, MCOs, and MAs. When an audit contractor references the wrong policy or audits outside of its scope, it can be incredibly disruptive for DMEPOS suppliers. Responding to such audits can be disruptive to business operations as it requires staff to divert from patient care. The repercussions from a bad audit can be significant such as a deactivation or revocation. To improve program integrity while minimizing burden on legitimate suppliers, all audit contractors should be required to apply coverage and documentation policies consistently and conduct their audits within their scope of work. For example, for fraud-focused auditors such as UPICs, their workloads should be focused on suppliers with suspicious activity rather than auditing suppliers that have already successfully passed audits from other contractors. Greater coordination among auditing entities, supported by adequately trained and knowledgeable staff, would improve efforts on combating fraud and abuse.

Improve Oversight and Reporting of Third-Party Administrators in MA and MCO

Vertical integration, such as health plans acquiring DMEPOS suppliers, and the expanding role of third-party administrators (TPAs) raise significant concerns related not only to market distortion but also to increased vulnerability to fraud, waste, and abuse. TPAs that administer benefits on behalf of MA and MCO plans often introduce additional administrative layers that obscure transparency. This lack of visibility, combined with complex billing systems and inconsistent policy requirements, makes it more difficult to identify irregularities, inflates administrative costs, and creates opportunities for fraudulent activity to go undetected. Like the challenges posed by pharmacy benefit managers (PBMs), TPAs act as intermediaries that can disrupt clear lines of accountability, impede oversight, and negatively affect patient care.

To strengthen fraud prevention efforts, we recommend that CMS enhance its oversight of vertically integrated health plans and the TPAs operating within them. CMS should require MA organizations to demonstrate that their integrated arrangements do not restrict patient access, inflate costs, or create conditions that heighten fraud risk. We also urge CMS to mandate that TPAs and managed care organizations adopt uniform claim reporting standards, including consistent data elements, definitions, file layouts, and submission timelines. Standardization will reduce discrepancies that obscure fraudulent patterns and will enable more accurate, apples-to-apples comparisons across plans.

Such consistent reporting should support near-real-time monitoring of utilization trends, flag anomalies, detect potential fraud earlier, track prior authorization outcomes, and evaluate network adequacy. Uniform transparent data processes are essential to strengthening program integrity and closing gaps that currently allow fraudulent activities to persist.

Conclusion

AAHomecare remains a devoted partner in the shared mission to protect the integrity of the Medicare program and its trust fund dollars, while ensuring that beneficiaries maintain access to essential equipment. We support a comprehensive but targeted strategy that includes strengthening provider enrollment and leveraging technology to identify and prevent fraudulent entities from entering the Medicare market.

By working together, we can make strides in ensuring bad actors do not take advantage of the Medicare program while supporting the thousands of legitimate suppliers who are committed to supporting patients in their homes.

We appreciate the opportunity to provide these comments. Please contact me at tomr@aahomecare.org for further information.

Sincerely,

Thomas Ryan
President and CEO
American Association for Homecare