United States Government Accountability Office

Report to the Chairman
Special Committee on Aging
United States Senate

March 2026

# MEDICARE

# CMS's Use of Data Analytics to Identify and Prevent Fraud



GAO-26-107799

GAO Highlights

MEDICARE

# CMS's Use of Data Analytics to Identify and Prevent Fraud

GAO-26-107799 March 2026

A report to the Chairman, Special Committee on Aging, United States Senate

For more information, contact: Leslie V. Gordon, GordonLV@gao.gov, or Seto J. Bagdoyan, BagdoyanS@gao.gov

## What GAO Found

GAO has designated Medicare a high-risk program due, in part, to its complexity and potential for fraud. Fraud schemes in traditional Medicare often focus on certain services, such as durable medical equipment. Fraudsters may use stolen or inappropriately obtained Medicare beneficiary identifiers to submit fraudulent claims for unneeded or never provided services.

The Centers for Medicare & Medicaid Services (CMS), which oversees Medicare, uses data analytics on claims in traditional Medicare to identify anomalous patterns indicative of emerging fraud schemes and potentially fraudulent behaviors, such as billing spikes. CMS uses these analytics to develop leads for investigations and to inform administrative actions that can prevent potentially fraudulent payments, such as suspending provider payments. For example, in 2023 and 2024, CMS suspended payments to, and later revoked the enrollment of, 15 providers involved in a scheme that allegedly billed Medicare for more than $4 billion in urinary catheters that were never supplied. Selected private payers GAO spoke with reported using data analytics in ways similar to CMS—namely, to identify anomalous provider billing patterns to generate leads for investigations and to inform actions like payment suspensions.

CMS estimates that from fiscal years 2022 through 2024, it prevented a total of $11.9 billion in potentially fraudulent Medicare payments by taking administrative actions on providers engaged in potential fraud.

**Administrative Actions and Estimates of Potentially Fraudulent Payments Prevented by CMS, Fiscal Years 2022 through 2024**

| Administrative action | Prevented payments (in millions) |
|---|---|
| Prepayment claims reviews | $27 |
| Automated prepayment denials | $132 |
| Overpayment recoveries | $652 |
| Payment suspensions | $2,579[a] |
| Revocations and deactivations | $7,962[a] |
| Law enforcement referrals | $554[b] |
| **Total** | **$11,906** |

Source: GAO analysis of Centers for Medicare & Medicaid Services (CMS) data. | GAO-26-107799
Note: For more details, see Table 3 in GAO-26-107799.
[a]Projected amount of potentially fraudulent payments prevented based on estimated cost avoidance.
[b]Estimated amount in financial judgments that courts may order on behalf of Medicare.

In December 2025, CMS began sharing information about Medicare provider payment suspensions with supplemental payers—private plans and state Medicaid agencies that cover certain Medicare beneficiaries' out-of-pocket expenses. CMS did not share such information previously. This lack of information sharing led some supplemental payers to pay beneficiary cost sharing on potentially fraudulent claims. Representatives of private payers estimated that private plans may have paid tens of millions of dollars in beneficiary cost-sharing for the urinary catheter scheme. GAO's analysis found that state Medicaid agencies paid at least $196,000 in state and federal funds for cost-sharing payments for the urinary catheter scheme in 2023 and 2024.

## Why GAO Did This Study

CMS is responsible for ensuring the integrity of the Medicare program and preventing and mitigating potential fraud.

GAO was asked to review CMS's use of data analytics to prevent and reduce fraud in traditional Medicare. This report describes characteristics of common Medicare fraud schemes, CMS's use of data analytics to identify Medicare fraud, and CMS's estimates of potentially fraudulent payments it prevented; and examines the extent to which CMS shares information on payment suspensions with relevant entities.

GAO reviewed CMS documentation on its activities to prevent fraud and interviewed CMS officials and program integrity contractors that investigate Medicare fraud about common Medicare fraud schemes and their use of data analytics. GAO also analyzed CMS data on administrative actions and the extent of potentially fraudulent payments prevented for fiscal years 2022 through 2024. Data from 2024 were the most recent data available at the time of GAO's review.

For additional context on CMS's use of data analytics, GAO interviewed representatives of selected private health insurers and two organizations representing private payers about their use of data analytics. GAO also interviewed CMS officials and private payers about the sharing of information on payment suspensions with supplemental payers.

The Department of Health and Human Services provided technical comments, which GAO incorporated as appropriate.

# Contents

Figures



**Abbreviations**

| | |
|---|---|
| AI | artificial intelligence |
| CMS | Centers for Medicare & Medicaid Services |
| DME | durable medical equipment |
| DOJ | Department of Justice |
| FPS | Fraud Prevention System |
| Fraud Risk Framework | GAO's guide, *A Framework for Managing Fraud Risks in Federal Programs* |
| HHS | Department of Health and Human Services |
| HHS-OIG | Department of Health and Human Services Office of Inspector General |
| MBI | Medicare beneficiary identifier |
| OMB | Office of Management and Budget |
| UPIC | Unified Program Integrity Contractor |

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 30, 2026

The Honorable Rick Scott
Chairman
Special Committee on Aging
United States Senate

Dear Chairman Scott:

Medicare is the largest federal health program by expenditures, and it has a significant effect on the entire health care sector. In 2024, the Medicare program spent an estimated $1.1 trillion to provide health care services for approximately 68 million elderly and disabled individuals. Over the next decade, spending is expected to increase significantly as the U.S. population ages and more individuals receive Medicare benefits. The Medicare program pays more than one billion claims annually to more than 1.4 million providers through more than 20 different payment systems.

Due to Medicare's size and complexity and the potential for improper payments, fraud, waste, and abuse, we first designated Medicare a high-risk program in 1990.[1] The sheer amount of payments in the Medicare program creates significant fraud risks, and there have been numerous convictions for multimillion dollar schemes defrauding the program.[2] For example, in 2025, a Florida man was sentenced to 12 years of imprisonment and ordered to pay over $21 million in restitution for

[1]For the most recent High-Risk report, see GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

An improper payment is any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements.

Fraud involves obtaining a thing of value through willful misrepresentation characterized by making material false statements of fact based on actual knowledge, deliberate ignorance, or reckless disregard of falsity. Whether an act is in fact fraud is a determination that is made through the judicial or other adjudicative system. While all fraudulent payments are considered improper, not all improper payments are due to fraud. See GAO, *Improper Payments and Fraud: How They Are Related but Different*, GAO-24-106608 (Washington, D.C.: Dec. 7, 2023).

[2]There currently are no reliable estimates of fraud in Medicare. We have ongoing work examining the feasibility of such an estimate.

obtaining nearly $27 million in fraudulent Medicare payments for medically unnecessary durable medical equipment (DME).[3]

The Centers for Medicare & Medicaid Services (CMS)—the agency within the U.S. Department of Health and Human Services (HHS) that administers the Medicare program—is responsible for ensuring the integrity of the Medicare program and preventing and mitigating potential fraud. In traditional Medicare, the program generally makes payments directly to health care providers, such as hospitals, physicians, and DME suppliers, based on the claims that they submit for services that they render to beneficiaries. This is known as fee-for-service. CMS conducts data analyses on claims as part of its program integrity activities, which are designed to identify and prevent improper and potentially fraudulent payments, as well as to generate leads for anti-fraud investigations. Any providers that are determined by CMS to be engaged in potential fraud may be referred to law enforcement agencies—namely the HHS Office of Inspector General (HHS-OIG)—or face administrative actions by CMS, such as payment suspensions or revocation from the program.

A recent case involving the inappropriate billing of urinary catheters highlights both the risks Medicare faces and the program's efforts to prevent fraud. In 2023 and 2024, a group of 15 providers allegedly attempted to bill Medicare for more than $4 billion for catheters that were not needed and never provided to Medicare beneficiaries, according to CMS. Through early identification of the scheme, CMS implemented payment suspensions that the agency said prevented over 99 percent of the payments from being made.[4]

[3]See *United States v. Roussonicolos, et al*, No. 21-cr-60273 (S.D. F.L. July 1, 2025). DME refers to equipment and supplies ordered by a health care provider for everyday or extended use, such as oxygen equipment and wheelchairs.

[4]See Department of Health and Human Services, Centers for Medicare & Medicaid Services, *Urinary Catheter Case Study: CMS' Swift Action Saves Billions,* Sept. 23, 2024. CMS may suspend Medicare payments in whole or in part in certain circumstances, such as upon making a determination that a credible allegation of fraud exists against a provider or supplier. 42 C.F.R. § 405.371.

You asked us to review CMS's use of data analytics in traditional Medicare to prevent and reduce fraud.[5] This report:

1. describes characteristics of common Medicare fraud schemes;
2. describes CMS's use of data analytics to identify, prevent, and mitigate Medicare fraud;
3. examines the extent to which CMS shares information on payment suspensions with relevant entities; and
4. describes CMS's estimates of the amount of potentially fraudulent payments that it prevented in fiscal years 2022 through 2024.

To describe characteristics of common Medicare fraud schemes, we reviewed HHS, CMS, and Department of Justice (DOJ) documentation.[6] We interviewed CMS and HHS-OIG officials and representatives from all five Unified Program Integrity Contractors (UPIC)—program integrity contractors responsible for identifying and investigating potential Medicare fraud—about common Medicare schemes. In addition, to provide further context on how fraudsters could obtain information needed to commit Medicare fraud, we reviewed "dark web" marketplaces and made two separate purchases of beneficiaries' personally identifiable information, including confidential Medicare beneficiary identifiers (MBI).[7]

To describe CMS's use of data analytics to identify, prevent, and mitigate Medicare fraud, we reviewed CMS documentation on the data analytic systems used by the agency to identify and track potentially fraudulent Medicare payments. We interviewed CMS officials and UPIC representatives on how they use data analytics to mitigate fraud. We also reviewed CMS documentation on the agency's process for assessing the Fraud Prevention System (FPS)—a data analytic system used by CMS

[5]The scope of this report is limited to traditional Medicare, covering inpatient, outpatient, physician and clinician services as well as DME supplies, paid on a fee-for-service basis. We did not include either Medicare Advantage, the private plan alternative, because it involves a different payment system, or the Medicare Part D prescription drug benefit.

[6]For the purposes of our analysis, a fraud scheme is defined as alleged or adjudicated illegal conduct involving misrepresentation carried out against Medicare using one or more processes, techniques, or systems for profit or other gain.

[7]The "dark web" is a hidden part of the internet that users access using specialized software. We referred information on our purchases to HHS-OIG for possible further investigation.

and UPICs to identify potential fraud. For additional context on CMS's use of data analytics, we interviewed a nongeneralizable selection of representatives of five private payers and two organizations representing private payers about their use of data analytics, and three information technology vendors.

To examine the extent to which CMS shares information on payment suspensions, we interviewed CMS officials on agency processes for sharing information on payment suspensions with supplemental payers—private Medigap plans and state Medicaid agencies that cover certain Medicare beneficiaries' out-of-pocket expenses.[8] We also interviewed representatives of private payers and private payer associations and obtained estimates of supplemental payments made to the providers whose payments were suspended for involvement in the urinary catheter scheme. We analyzed Transformed Medicaid Statistical Information System data on Medicaid payments to 15 providers involved in the scheme and determined that the data were sufficiently reliable for the purposes of our report. We evaluated CMS's information sharing against a relevant leading practice identified in *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework) to establish collaborative relationships with relevant external entities.[9]

To describe CMS's estimates of the amount of potentially fraudulent payments that it prevented in fiscal years 2022 through 2024, we obtained and analyzed CMS data for those years on administrative actions taken, and the associated amounts of potentially fraudulent payments that were prevented.[10] We determined that the data were sufficiently reliable for the purposes of our report. See appendix I for more information about our objectives, scope, and methodology.

We conducted this performance audit from September 2024 to March 2026 in accordance with generally accepted government auditing

[8]Medicare beneficiaries may purchase supplemental coverage from private health insurance plans, called Medigap. Medicaid is a joint federal-state program that finances health care for low-income and medically needy individuals.

[9]See GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

[10]Throughout this report, we use the term "potentially fraudulent payments" to refer to improper payments identified through CMS's and the UPICs' anti-fraud activities.

Data from 2024 was the most recent data available at the time of our review, and we also reviewed data from 2022 and 2023 for additional context.

standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additionally, our related investigative work was conducted in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

# Background

## Medicare Program Integrity Activities

CMS conducts a variety of activities to support the agency's Medicare program integrity efforts. This includes activities directed at ensuring compliance with Medicare coverage and payment requirements, reducing improper payments, and preventing potential fraud. For example, CMS processes claims for traditional Medicare, identifies areas vulnerable to improper billing, and develops general education efforts focused on these areas.[11]

As part of processing claims, CMS executes prepayment edits—automated controls applied to all Medicare claims that deny claims that do not comply with Medicare requirements. For example, some edits deny claims that do not contain all required data elements. Other edits enforce coverage requirements and may help prevent improper payments, such as edits that deny claims for services that should not be billed together.

An additional way CMS helps ensure claims comply with Medicare coverage requirements is through prepayment claims reviews, which involve manual medical record reviews of claims prior to payment. Many improper or potentially fraudulent claims can be identified only by manually reviewing associated medical records and beneficiary claim histories and exercising clinical judgment to determine whether services were reasonable and necessary. For these reviews, providers are required to submit beneficiary medical records associated with the claims under review. CMS then employs trained clinicians and coders to examine the claims and medical records to ensure that the claims comply

[11]CMS uses a variety of contractors to support its program integrity activities, including Medicare administrative contactors, UPICs, and recovery auditors.

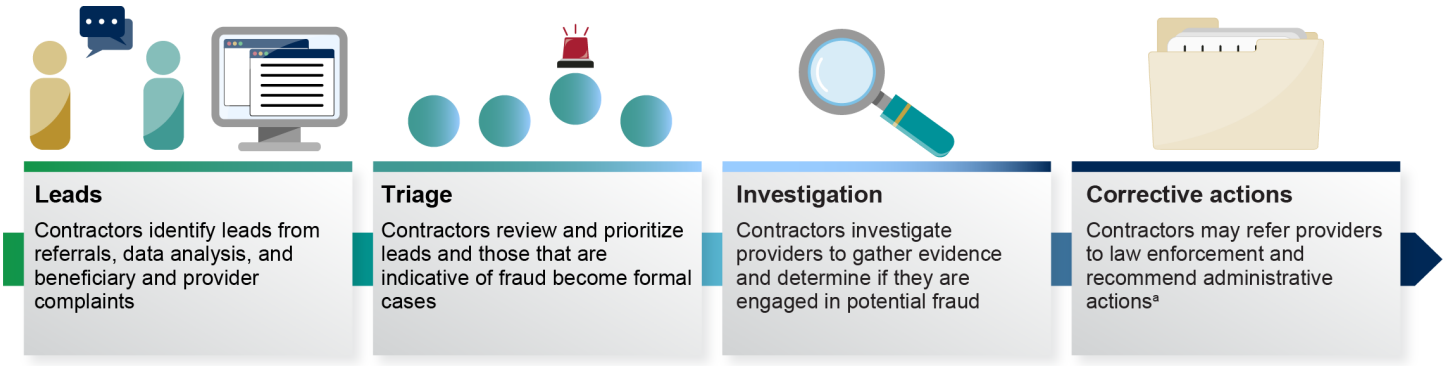
with Medicare coverage requirements.[12] Generally, less than 1 percent of claims are subject to claim reviews, though CMS may subject all of a given provider's claims to review in response to improper billing or potentially fraudulent behavior.

## Unified Program Integrity Contractors

One component of CMS's Medicare program integrity efforts specifically focuses on activities to identify and investigate potentially fraudulent behavior and stop potentially fraudulent payments. CMS contracts with UPICs that operate in five geographic jurisdictions to support the agency's efforts to identify and investigate providers engaged in potential Medicare fraud. In fiscal years 2022 through 2024, CMS's contract obligations to the UPICs averaged $137 million annually.[13]

The UPICs identify leads for potential provider investigations from a variety of sources, including referrals and data analysis. A number of entities, including CMS, law enforcement agencies, and other Medicare contractors, refer leads about suspect providers to the UPICs. The UPICs may also develop leads based on beneficiary and provider complaints and allegations. See figure 1 for information on UPIC investigation processes.

**Figure 1: Unified Program Integrity Contractor Investigation Process**




Source: GAO analysis of Centers for Medicare & Medicaid Services information; GAO (icons). | GAO-26-107799

[12]For example, CMS officials may check beneficiary medical records and diagnoses to determine eligibility for home health services when reviewing claims for home health care. For additional information on Medicare claim reviews, see GAO, *Medicare: Claim Review Programs Could Be Improved with Additional Prepayment Reviews and Better Data*, GAO-16-394 (Washington, D.C.: Apr. 13, 2016).

[13]In addition to preventing potential Medicare fraud, the UPICs are also responsible for conducting activities to prevent and reduce Medicaid fraud. The contract obligations include both Medicare and Medicaid activities.

[a]Administrative actions include suspending provider payments and revoking providers' Medicare enrollment, among other actions.

UPICs generally have a triage process to review leads and determine whether the leads are indicative of fraud. If fraud is suspected, they initiate a case to investigate the provider. These investigations can involve conducting beneficiary and provider interviews, site visits of provider facilities, and manual reviews of provider claims. If UPICs uncover evidence of potential fraud, they refer the investigation to the HHS-OIG for further examination, which may lead to possible criminal or civil prosecution by DOJ. Additionally, the UPICs may recommend a range of administrative actions to CMS, such as revoking providers' enrollment from the program.

## Key Medicare Fraud Statutes and Mechanisms for Committing Medicare Fraud

Medicare fraud may take several forms. This includes fraudulent billing for services or items not provided; providing or supplying services or items that were not medically necessary; and intentionally billing services at a higher payment level than provided or appropriate. In some instances, Medicare fraud also involves providing compensation—kickbacks—to providers, beneficiaries, or others for participating in the fraud.

Medicare fraud may involve violations of multiple federal statutes, including but not limited to the following three statutes.[14]

- **The civil False Claims Act** is often used by the federal government in Medicare fraud cases and prohibits certain actions, including the knowing presentation of a false claim for payment by the federal government.[15]
- **The Social Security Act** contains provisions that apply civil monetary penalties to certain activities, such as knowingly presenting a claim for medical services under a federal health care program that is known to be false or fraudulent.[16] In addition, the Social Security Act stipulates

[14]The statutes included here provide examples of those that may be relevant to health care fraud cases. Other statutory provisions, including those located in title 18 of the United States Code, may also be relevant to such cases. See, e.g., 18 U.S.C. §§ 669 (concerning theft or embezzlement in connection with a health care benefit program), 1035 (concerning false statements relating to any matter involving a health care benefit program), and 1347 (concerning health care benefit program fraud).

[15]31 U.S.C. §§ 3729-3733.

[16]42 U.S.C. § 1320a-7a.

criminal penalties for knowing and willful false statements in applications for payment under a federal health care program.[17]

- **The Anti-Kickback statute** makes it a criminal offense for anyone to knowingly and willfully solicit, receive, offer, or pay any remuneration in return for or to induce referrals of items or services reimbursable under a federal health care program, subject to statutory exceptions and regulatory safe harbors.[18]

GAO created an anti-fraud resource to help federal programs identify the key aspects of fraud schemes that target federal programs or operations.[19] The resource outlines several mechanisms that a fraudster may use to commit health care fraud. A given Medicare fraud case or scheme could involve several of these mechanisms. These mechanisms include but are not limited to the following:

- **Misrepresentation:** False statements of a material fact in seeking payments, such as submitting fraudulent Medicare claims or fraudulent documentation to support a claim.
- **False claims:** Claims for expenses not incurred, for services not rendered, or for items not delivered.
- **Billing manipulation:** Intentional and systemic submission of claims for services beyond those that were provided or appropriate.[20]

[17]42 U.S.C. § 1320a-7b.

[18]42 U.S.C. § 1320a-7b(b). Kickbacks are a type of illegal remuneration under the statute. Examples of kickbacks include providing identifying information to a provider allowing the provider to bill for services not provided, receiving services in exchange for cash, or compensating individuals for recruiting beneficiaries to receive treatment at a specific clinic.

[19]All federal fraud schemes include five key aspects: (1) a federal program or operation affected by the fraud, (2) a participant involved in the fraud, (3) the fraud activity committed, (4) the mechanism used to achieve the fraud, and (5) the impact of the fraud. For more information, see GAO, *Antifraud Resource,* (Washington, D.C.: Jan. 10, 2022), https://antifraud.gaoinnovations.gov/howfraudworks.

[20]For example, a fraudster may intentionally and systematically overstate the level of services performed or the severity of beneficiaries' conditions to increase reimbursement amounts. This may also involve intentionally and systemically billing separately for services that should be billed together.

- **Medical identity fraud:** The misuse of a beneficiary's medical information, including name and MBI, to fraudulently file claims.[21]

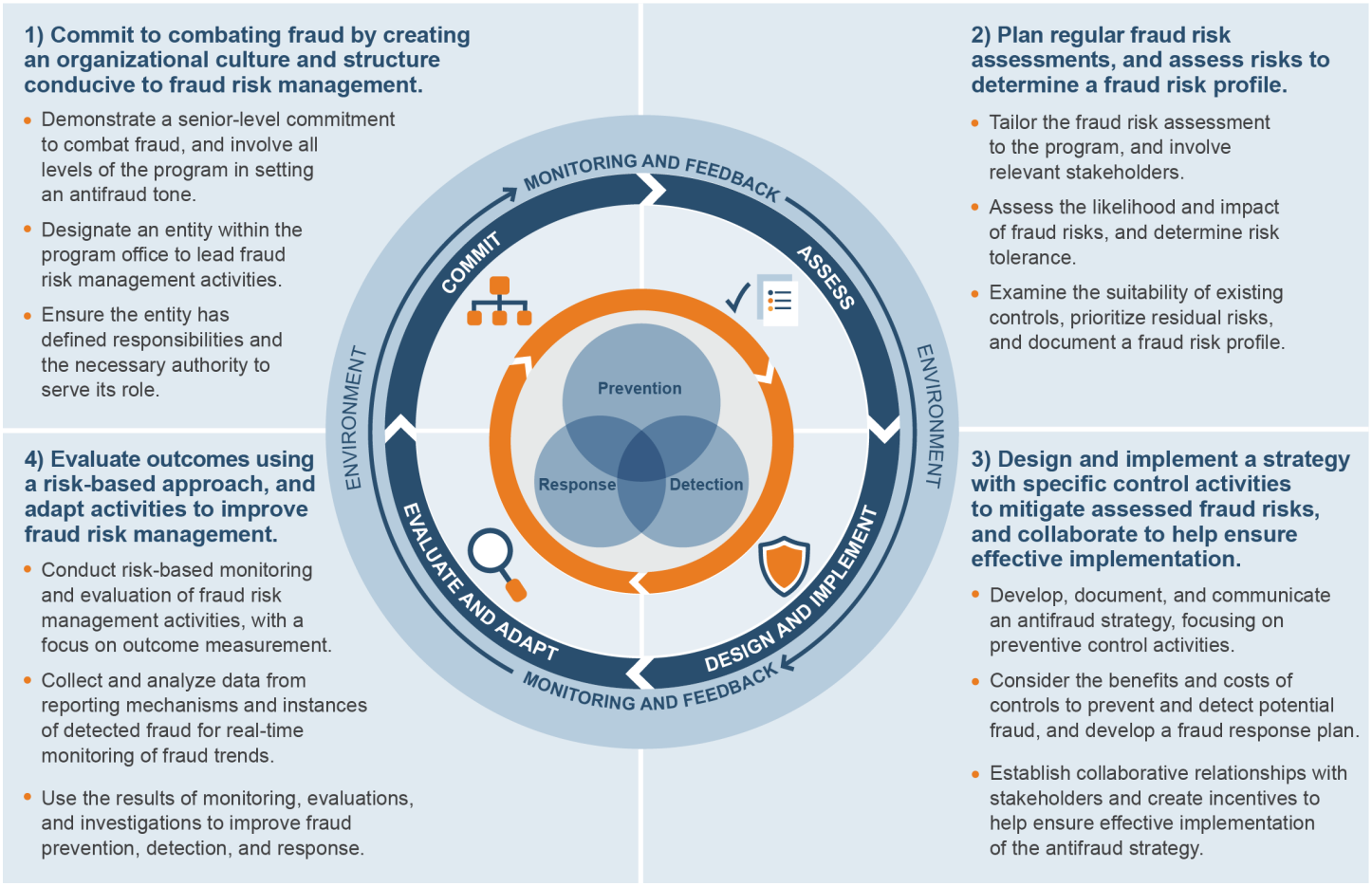
## Fraud Risk Management

Federal agencies are responsible for managing fraud risks and implementing practices for mitigating those risks. Issued in 2015, the Fraud Risk Framework is a set of leading practices that serves as a guide for combating fraud in a strategic, risk-based manner.[22] As depicted in figure 2, the framework organizes the leading practices within four components: (1) Commit, (2) Assess, (3) Design and Implement, and (4) Evaluate and Adapt. One of the leading practices in the third component is to establish collaborative relationships with relevant external entities, including sharing information on fraud risks.

[21]MBIs are unique and confidential beneficiary identifiers that are used for Medicare transactions. For example, providers are required to include MBIs to submit claims to Medicare.

[22]GAO-15-593SP.

**Figure 2: GAO's Fraud Risk Management Framework**




Source: GAO (information and icons). | GAO-26-107799

In June 2016, the Fraud Reduction and Data Analytics Act of 2015 required the Office of Management and Budget (OMB) to establish guidelines for federal agencies to create controls to identify and assess fraud risks to design and implement antifraud control activities. The act further required OMB to incorporate the leading practices from the Fraud Risk Framework in the guidelines.[23] The Payment Integrity Information Act of 2019 repealed the Fraud Reduction and Data Analytics Act of 2015

[23]Pub. L. No. 114-186, 130 Stat. 546 (2016).

but maintained the requirement for OMB to provide guidelines to agencies in implementing the Fraud Risk Framework.[24]

In its 2016 Circular No. A-123 guidelines, OMB directed agencies to adhere to the Fraud Risk Framework's leading practices.[25] In October 2022, OMB issued a Controller Alert reminding agencies that they must establish financial and administrative controls to identify and assess fraud risks.[26] In addition, the alert reminded agencies that they should adhere to the leading practices in the Fraud Risk Framework as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks.

## Medicare Supplemental Payers

Most traditional Medicare beneficiaries have some form of additional health care coverage—referred to as supplemental coverage—to help them pay their cost sharing.[27] This includes their 20 percent coinsurance for certain Medicare services, such as DME (see fig. 3). In 2022, 77 percent of beneficiaries had supplemental coverage through a private supplemental payer. This includes coverage purchased from private Medigap plans and coverage received by certain retirees through a former employer. In addition, beneficiaries eligible for both Medicare and Medicaid may receive supplemental coverage through Medicaid. In 2022, 11 percent of Medicare beneficiaries had such coverage through Medicaid.[28]

[24]Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131–132 (2020), codified at 31 U.S.C. § 3357. The act requires these guidelines to remain in effect, subject to modification by OMB as necessary and in consultation with GAO.

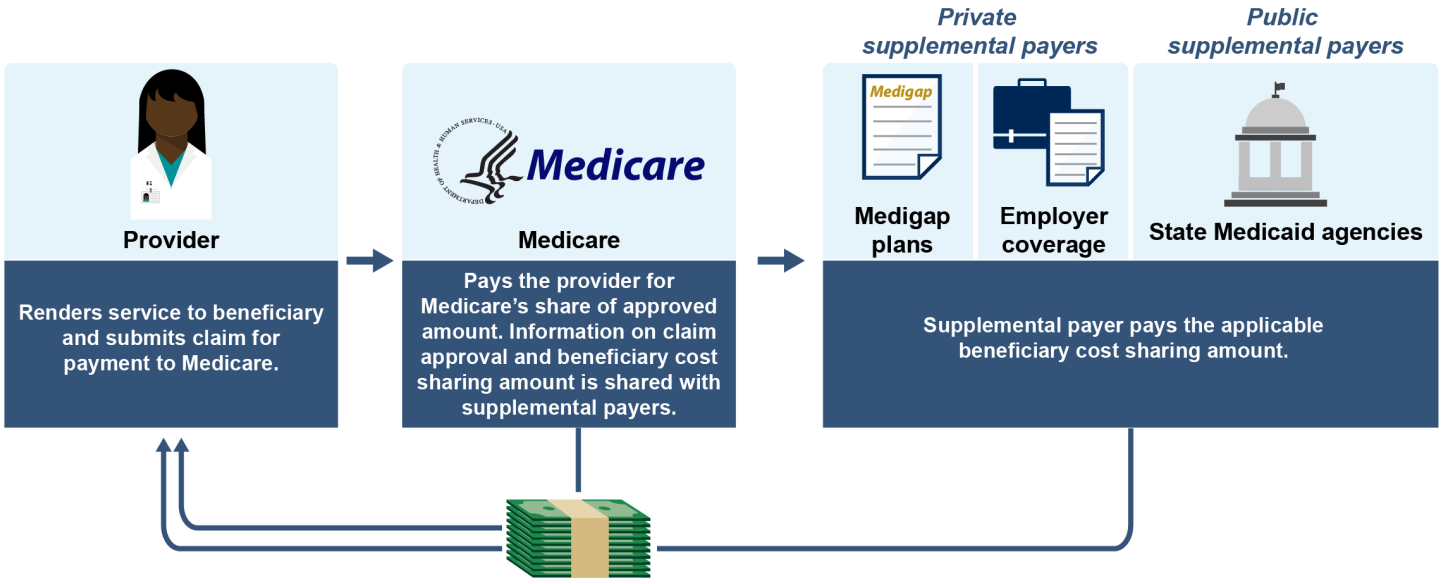
[25]See Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular No. A-123 (Washington, D.C.: July 15, 2016).

[26]See Office of Management and Budget, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk*, CA-23-03 (Washington, D.C.: Oct. 17, 2022).

[27]Cost sharing is the portion of costs that beneficiaries are expected to pay, such as deductibles, coinsurance, and co-payments.

[28]See MedPAC, *A Data Book: Health care spending and the Medicare program, July 2025*, "Section 3: Medicare beneficiary and other payer financial liability" (Washington, D.C.: July 17, 2025). The percentages are for noninstitutional beneficiaries, and 2022 is the most recent year for which data are available.

**Figure 3: Medicare Supplemental Payments**




Source: GAO analysis of Centers for Medicare & Medicaid Services information; GAO (icons). | GAO-26-107799

Note: Supplemental payers help Medicare beneficiaries pay their cost sharing, such as their 20 percent coinsurance for certain Medicare services. Beneficiaries can purchase supplemental coverage through private Medigap plans or may receive coverage from a former employer. Beneficiaries eligible for both Medicare and Medicaid may receive supplemental coverage through Medicaid, a joint federal-state program that finances health care for low-income and medically needy individuals.

## Characteristics of Medicare Fraud Schemes Include Inappropriate Use of Billing Privileges and Beneficiary Identifiers

Based on our review of agency documentation; interviews with CMS and HHS-OIG officials, and UPIC representatives; and our review of examples of Medicare fraud cases, we found that many Medicare fraud schemes depend on the inappropriate use of multiple elements. These include (1) Medicare provider billing privileges, (2) Medicare beneficiary identifiers, (3) provider orders, and (4) targeted services.

**Medicare provider billing privileges.** To defraud Medicare as a provider, fraudsters need to gain Medicare billing privileges themselves or through a proxy. According to UPIC representatives, fraudsters often gain Medicare billing privileges by enrolling as certain types of providers, such as DME suppliers. In recent years, fraudsters in certain western states have enrolled as hospices as another method of gaining Medicare billing privileges. Representatives of a UPIC that has experienced high levels of hospice fraud noted cases in which multiple nonoperational hospices have enrolled in Medicare using the same address, but different suite numbers. Since hospice care is often provided in beneficiaries' homes,

hospices are not necessarily expected to maintain a significant physical presence or medical facility.

**Example of Fraud Case Involving the Misapplication of Medicare Billing Privileges**

According to DOJ, a Florida man owned and operated five durable medical equipment (DME) suppliers as a silent partner. He was ineligible to enroll in Medicare as a provider because he had one or more felony convictions. He instead recruited and paid co-conspirators to serve as nominal owners of the DME suppliers and led others to falsify Medicare enrollment forms, bank records, and other documents to conceal the true ownership and control of the DME suppliers. In 2025, he was sentenced to 12 years in prison and ordered to pay $21 million in restitution.

Source: GAO analysis of Department of Justice (DOJ) information. | GAO-26-107799

Representatives from one UPIC noted that, in some cases, fraudsters have purchased existing provider companies already enrolled in Medicare to obtain billing privileges. Medicare providers are required to report changes in enrollment information, and new owners are required to submit appropriate enrollment applications. However, representatives from that UPIC also told us that such reporting does not always occur, especially in cases related to potential fraud. For example, the alleged fraudsters who attempted to bill Medicare for $4 billion in urinary catheters did so after they purchased existing DME provider companies with Medicare billing privileges, according to DOJ.[29]

**Medicare beneficiary identifiers.** The misuse of stolen or inappropriately obtained MBIs is often a critical component of fraud schemes, as MBIs are a required element on claims for payment. Fraudsters may steal or otherwise inappropriately obtain these MBIs in several ways. One way is through data breaches of entities that handle MBIs and beneficiaries' personally identifiable information. Another way is through cold calls to beneficiaries to get their personally identifiable information or to convince them to obtain services they do not need. For example, some fraudsters have employed telemarketers to convince beneficiaries to request unneeded DME items. Fraudsters have also accessed beneficiary information by exploiting MBI lookup tools created to assist providers. In certain instances, beneficiaries have been recruited and offered kickbacks to participate in schemes.

[29]See Department of Justice, Press Release, *National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud*, June 30, 2025.

**Example of Fraud Case Involving Misappropriated Medicare Beneficiary Identifiers**

According to DOJ, a foreign national obtained Medicare beneficiary identification cards and knowingly sold Medicare beneficiaries' personal information to a durable medical equipment company that used the information to submit fraudulent claims to Medicare. The durable medical equipment company used the information to bill Medicare for orthotic braces that were never provided. In 2025, he was sentenced to 30 months in prison and ordered to pay almost $1.5 million in restitution.

Source: GAO analysis of Department of Justice (DOJ) information. | GAO-26-107799

In addition, confidential MBIs and other content needed to commit fraud can be purchased from online marketplaces. Our purchases of MBIs on the dark web exemplify how such information is available to fraudsters. In particular, we posed as fraudsters to make two separate purchases of beneficiaries' personally identifiable information, including corresponding MBIs, that could be used to fraudulently submit claims. For one purchase, we received a data set containing beneficiaries' information. For the other purchase, we received pictures of the beneficiaries' identification cards. We referred the contact information of the sellers and the information we received from them to the appropriate law enforcement officials.

**Example of a Fraud Case Involving the Misuse of Provider Orders**

According to DOJ, a Texas doctor signed thousands of medical records and orders for orthotic braces and genetic tests that falsely represented that the braces and tests were medically necessary. He falsely stated that he diagnosed the beneficiaries, had a plan of care for them, and recommended that they receive certain additional treatment. In 2025, he was sentenced to 10 years in prison and ordered to pay $26 million in restitution.

Source: GAO analysis of Department of Justice (DOJ) information. | GAO-26-107799

**Provider orders.** To be covered by Medicare, services such as DME or laboratory tests generally require an order from a provider for a medically necessary service or item. For example, a provider needs to diagnose a beneficiary with diabetes and provide the appropriate order for beneficiary coverage of diabetic testing strips from a DME supplier. Medicare claims for such services are required to include the provider identifier of the ordering provider. Fraudsters can obtain orders by misappropriating the information of an uninvolved and unwitting provider, collaborating with a conspiring practitioner, or by purchasing fraudulent orders.

**Targeted services.** Schemes tend to target services or supplies, such as certain DME products. In some instances, targeted services may be those that lack defined coverage or utilization policies that impose standards on when the services are covered by Medicare. For example, representatives from a UPIC said the lack of defined coverage policies for the use and application of high-reimbursement skin substitute products led to such products being used when not medically necessary and made them a target for fraud.[30]

[30]For more information on potential fraud related to skin substitute products, see OIG, *Medicare Part B Payment Trends for Skin Substitutes Raise Major Concerns About Fraud, Waste, and Abuse*, OEI-BL-24-00420 (Washington, D.C.: Sept. 3, 2025).

**Example of a Fraud Case Involving the Misapplication of a Targeted Service**

According to DOJ, an Arizona couple received more than $600 million in fraudulent payments from public and private payers, including Medicare, for the application of medically unreasonable or unnecessary skin substitute products. This involved applying the products to already healed wounds and infected wounds requiring differing treatments. The couple also received illegal kickbacks from a distributor of such products. In 2025, the wife and husband were sentenced to 15.5 and 14 years in prison respectively, ordered to pay Medicare a combined $594 million in restitution, and ordered to pay a combined $309 million in civil liabilities.

Source: GAO analysis of Department of Justice (DOJ) information. | GAO-26-107799

UPIC representatives noted that fraudsters may adapt their schemes by changing the services they target after CMS or UPICs identify and investigate the fraud schemes. Additionally, other UPIC representatives told us that fraud schemes that target certain services often develop regionally. Once a scheme is caught in one area, it may migrate to another part of the country.

CMS has taken steps to address the characteristics of fraud described above, including the following:

- CMS has implemented controls to help prevent fraudsters from enrolling as new providers in Medicare. Since 2011, CMS has imposed more stringent enrollment requirements and screening processes on high-risk providers, such as DME suppliers. This includes conducting site visits and collecting fingerprints of owners of DME suppliers for criminal background checks.[31] In February 2026, CMS announced a six-month, nationwide moratorium on enrolling new DME providers in response to concerns about DME fraud.[32] CMS has also taken steps to address concerns that fraudsters are enrolling as hospice providers. In 2023, CMS conducted more than 7,000 unannounced site visits to every Medicare-enrolled hospice to confirm the address listed on its Medicare enrollment form.
- CMS has taken steps to address issues with misappropriated MBIs. CMS has a process for updating MBIs that are known to be compromised, such as MBIs associated with known data breaches or fraud schemes. In February 2025, the agency also sought public feedback on how to limit the use of MBI lookup tools to commit MBI theft.
- CMS has updated policies or payment methodologies for services targeted by fraudsters. For instance, in November 2025, CMS changed the payment methodology for skin substitute products starting January 1, 2026, in part to address concerns about abusive and noncompliant billing practices.[33]

[31]For additional information on Medicare enrollment requirements and processes, see GAO, *Medicare: CMS Needs to Address Risks Posed by Provider Enrollment Waivers and Flexibilities*, GAO-23-105494 (Washington, D.C.: Dec. 19, 2022).

[32]91 Fed. Reg. 9855 (Feb. 27, 2026).

[33]90 Fed. Reg. 49,266 (Nov. 5, 2025). See Centers for Medicare & Medicaid Services, Press Release, "CMS Modernizes Payment Accuracy and Significantly Cuts Spending Waste," Oct. 31, 2025.

**Example of a Fraud Case Involving an Organization Located Abroad**

According to DOJ, in the span of two months, a home health company billed Medicare for $2.8 million in services that were never provided and routed the funds to a shell corporation abroad. In 2023, the owner was sentenced to 9 years in prison and ordered to pay over $2.7 million in restitution.

Source: GAO analysis of Department of Justice (DOJ) information. | GAO-26-107799

In addition to the characteristics of fraud schemes, officials from HHS-OIG and CMS, and representatives of UPICs described three developments contributing to recent Medicare fraud schemes.

- Medicare has increasingly been targeted for fraud by organized criminal groups, including from abroad.[34] Foreign organized crime groups often work with a contact in the U.S. who serves as the nominal, or front owner of the Medicare provider. Medicare payments are made to the nominal owner and money is routed abroad.
- Fraudsters' adoption of artificial intelligence (AI) may allow them to scale Medicare fraud schemes quickly. For example, AI may be used to generate and submit large amounts of false claims and generate fake beneficiary medical records.
- There is an increasing prevalence of "bust-out" schemes in which fraudsters suddenly and rapidly submit a large volume of fraudulent claims, often for services that were never provided. These schemes involve quickly obtaining large amounts in fraudulent payments before Medicare contractors identify and prevent the potentially fraudulent payments. For example, the urinary catheter scheme involved the providers suddenly billing Medicare for extreme volumes of the supplies in a short window of time. (For additional information on how the urinary catheter scheme could have affected payments to certain providers, see app. II.)

[34]We previously reported on the role of organized criminal groups, including international groups, in defrauding the federal government. See GAO, *Fraud Risk in Federal Programs: Continuing Threat from Organized Groups Since COVID-19*, GAO-25-107508 (Washington, D.C.: July 10, 2025) and GAO, *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs*, GAO-23-105331 (Washington, D.C.: May 18, 2023).

# CMS Uses Data Analytics to Identify Anomalous Billing Patterns and Inform Actions Aimed at Preventing Potentially Fraudulent Payments

## CMS Uses Data Analytics to Identify Anomalous Billing Patterns Indicative of Fraud

CMS uses data analytics as part of its strategy to detect and mitigate Medicare fraud. Specifically, CMS and the UPICs employ data analytics to identify anomalous billing patterns that may be indicative of (1) emerging fraud schemes and (2) providers engaged in potentially fraudulent behaviors. In particular, analytics that focus on larger Medicare billing patterns, such as a sudden increase in the number of claims for a specific service or DME item, can help identify emerging fraud schemes. Analytics that focus on provider billing patterns, such as a sudden increase in the number of claims submitted by a specific provider, can identify providers engaged in potential fraud and serve as leads for UPIC fraud investigations. These data analytics are run using multiple types of models, developed from algorithms that review a set of data, including Medicare claims data.[35] The data analytic models generally do not focus on reviewing whether a specific, individual claim is potentially fraudulent. CMS officials have noted that the agency does not have the authority to deny an individual claim solely based on data analytics.[36]

There are two primary mechanisms through which CMS and the UPICs use data analytics to identify fraud schemes and generate leads on providers engaged in potential fraud for UPIC investigations: (1) CMS's Fraud Prevention System (FPS) and (2) the UPICs' internally developed data analytic models.

- **CMS's Fraud Prevention System.** CMS manages FPS, which uses data analytic models that identify anomalous provider billing patterns

[35]Models analyze both paid claims and submitted, unpaid claims. For example, to identify dramatic increases in billing, models need to compare incoming claims against past claims.

[36]See GAO, *Medicare: CMS Fraud Prevention System Uses Claims Analysis to Address* Fraud, GAO-17-710 (Washington, D.C.: Aug. 30, 2017).

that may be indicative of fraud to generate leads for the UPICs, among other things.[37] To do this, FPS assigns risk scores to individual providers based on their billing patterns and the likelihood that they are engaged in potential fraud.[38] According to UPIC representatives, FPS provides readily available leads to investigate, and the risk scores that FPS generates for providers can help the UPICs to prioritize and triage those leads.

- **UPICs' data analytic models.** In addition to FPS, the UPICs develop and run their own data analytic models for providers and for claims in their geographic jurisdiction. The UPICs' data analytics regularly monitor billing levels of high-risk services, such as DME, and also identify providers with anomalous billing patterns. UPIC representatives told us that they run these models both manually and automatically, with some reports running on a monthly or weekly basis and others running daily. The UPICs develop and run these analytic models in response to emerging fraud trends from law enforcement agencies or information sharing from other UPICs. For example, if another UPIC has identified an emerging fraud scheme in its jurisdiction, a UPIC may develop an analytic model to see whether the scheme is appearing in its jurisdiction.

The UPICs consider CMS's priorities and health care standards of practice in developing data analytics. In particular, according to UPIC representatives, UPICs base their analytics on an annual CMS "direction letter" that details the services that should be the focus of the UPICs' anti-fraud efforts. Among other things, the letter indicates which fraud schemes are of highest priority for the year.

FPS and the UPICs both run different types of models that employ analytic approaches to identifying anomalous billing patterns indicative of

[37]Another role of FPS is to execute certain prepayment edits that automatically deny payments for claims that do not comply with Medicare coverage requirements. CMS reported that these prepayment edits in FPS prevented $207 million in improper payments in fiscal year 2024. See CMS, *Justification of Estimates for Appropriations Committees: Fiscal Year 2026*. We previously reported that the edits in FPS function similarly to those in CMS's claims processing systems. FPS edits do not analyze individual claims to automatically deny payments based on the risk or the likelihood that they are fraudulent; they deny claims for noncompliance with Medicare coverage requirements. For our prior reports on FPS, see GAO-17-710; and GAO, *Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness*, GAO-13-104 (Washington, D.C.: Oct. 15, 2012).

[38]FPS analytic models are developed by a variety of contractors, including by a contractor that develops models for FPS and by the UPICs.

fraud, such as looking for billing spikes and anomalies in provider billing patterns compared to peers.[39] Other models estimate the likelihood of providers being engaged in fraud based on risk-scoring tools, or may generate information indicating that certain services were never provided. Certain models use forms of AI, such as machine learning, to analyze billing patterns.[40] See table 1 for information on the types of models used.

**Table 1: Examples of Data Analytic Models Employed by CMS to Identify Potential Medicare Fraud**

| Data analytic model | Description |
|---|---|
| Billing spikes | Identify sudden increases, or spikes, of specific services that may indicate fraud. |
| Peer-to-peer analysis | Compare providers' billing activities to peer providers—providers in the same specialty or geographic area—to detect anomalous patterns. |
| Risk scoring | Develop risk scores for providers based on their billing patterns and other information to estimate the likelihood of fraud. |
| Predictive analytics | Use historical data to identify anomalous billing patterns associated with fraud and then use it to identify potential fraud when applied to current claims data. |
| Unstructured machine learning | Use machine learning, a type of artificial intelligence, to analyze unstructured data and identify patterns of anomalous billing.[a] |
| Rules-based models | Identify potentially fraudulent claims and behaviors based on set thresholds or criteria, such as provider claims that exceed 24 hours of care in a single day. |
| Geographic provider analyses | Compare provider locations to the locations of beneficiaries to detect anomalies. |
| Peer network mapping | Provide a visual representation of relationships between providers to detect indications of collusion, such as potentially fraudulent collaboration between a referring and billing provider. |

Source: GAO analysis of Centers for Medicare & Medicaid Services (CMS) documents and interviews; interviews with Unified Program Integrity Contractors. | GAO-26-107799

[a]Unstructured data is primarily information that has not been organized into a structured format for analysis.

UPIC representatives also noted that the information provided by data analytics can be combined with information identified through other sources, such as fraud referrals, to help develop and guide investigative leads. For example, when the UPIC gets a fraud referral, UPIC staff will

[39]According to the UPIC representatives, the models are developed with input from subject matter experts, such as medical coders and health professionals, to help ensure that the identified anomalies are indicative of fraud rather than a more innocuous variation from typical billing patterns. For example, health professionals can discern when providers have increased their use of certain procedures or treatments, such as in response to seasonal illnesses, which would result in increases in billing that are expected or reasonable.

[40]We previously reported on the use of AI and other innovative technologies to combat fraud and improper payments. See GAO, *Fraud and Improper Payments: Data Quality and a Skilled Workforce Are Essential for Realizing Artificial Intelligence's Benefits,* GAO-26-108850 (Washington, D.C.: Jan. 13, 2026).

check whether any FPS models have identified the provider named as having anomalous billing patterns. The models are also designed to provide a road map for what evidence needs to be collected during an investigation to support the administrative action and potential law enforcement referrals. For example, models can point investigators to conduct interviews with providers and beneficiaries or review medical records to identify the scope of the fraud exposure.

## CMS Uses Data Analytics to Inform Administrative Actions Aimed at Preventing Potentially Fraudulent Payments

As part of CMS's fraud mitigation processes, the agency uses data analytics, including FPS and the UPICs' internally developed data analytic models, to inform administrative actions for providers with anomalous billing patterns and help prevent potentially fraudulent claims from being paid. These actions include putting providers on manual prepayment claim reviews, implementing payment suspensions while CMS conducts investigations, and revoking providers' enrollment from the program. See table 2 for more information on these administrative actions.

**Table 2: Medicare Administrative Actions**

| CMS action | Description |
|---|---|
| Prepayment claim review | Withholding of payments to providers pending manual medical record review of provider claims. Providers submit medical records to support their claims, and CMS examines the claims and medical records to ensure claims comply with Medicare coverage requirements. |
| Automated prepayment denials | Prepayment edits specific to individual providers that automatically deny payments to the provider, such as provider claims for a specific service. Also includes automated denials to providers under prepayment claim review that do not submit medical records to support their claims in a timely manner. |
| Overpayment recoveries | Collection of provider payments received in excess of amounts payable. |
| Payment suspension | Temporary suspension of provider payments to allow the agency to investigate credible information on potential fraud or overpayments.[a] |
| Revocation | Termination of provider's Medicare enrollment and billing privileges. |
| Deactivation | Deactivation, or pausing, of provider's Medicare billing privileges, which can be reactivated.[b] |

Source: GAO analysis of Centers for Medicare & Medicaid Services (CMS) information. | GAO-26-107799

[a]Referrals to law enforcement and additional administrative actions may be taken based on the outcome of the investigation.

[b]A deactivation can occur if a provider does not report changes in enrollment information in a timely manner or if a provider's practice location is non-operational, among other reasons. A provider can be reactivated upon submission of a new Medicare enrollment application or by recertifying that current enrollment information is correct.

UPIC representatives told us that data analytics are often designed to help inform and support effective investigations and quick administrative actions. For example, a UPIC model may detect that a certain provider has an unusual or suspect billing pattern consistent with known fraud schemes. Such identified patterns can help investigators quickly put a

provider on a payment suspension or prepayment claims review. In addition, CMS officials and UPIC representatives stated that, in response to the rise of bust-out schemes, starting in 2023, FPS and some UPICs began running data analytics on claims earlier in the claims processing process. According to the representatives, the earlier review of claims has allowed the UPICs to identify the billing spikes associated with bust-out schemes before claims are paid.

In addition, beginning in 2025, CMS launched an initiative, the Fraud Defense Operations Center, to leverage the agency's use of data analytics to mitigate fraud. According to CMS officials, the center brings together CMS subject matter experts and officials from law enforcement agencies to review anomalous provider billing patterns and make quicker determinations on administrative actions when potential fraud is suspected.

CMS and UPIC officials said that certain administrative actions—prepayment claim reviews and payment suspensions—are particularly effective at preventing potentially fraudulent claims from being paid in the first place. In response to anomalous provider billing patterns, providers may be put on prepayment claims reviews, in which payments are withheld and providers' claims are subject to medical review. Claims can be denied if providers do not respond to UPIC requests for medical records, or if reviews determine that the claims do not comply with Medicare coverage policies. CMS also uses payment suspensions to withhold payments to providers suspected of potential fraud, including to the 15 providers involved in the urinary catheter scheme. The payment suspensions allow the agency time to investigate the provider before making or denying payments.[41]

[41]See GAO-17-710. CMS data analytics generally do not focus on reviewing whether individual payments are potentially fraudulent, but instead focus on identifying and taking action against providers engaged in patterns of billing indicative of potential fraud. Payment denials of potentially fraudulent claims follow administrative actions taken against providers.

**Selected Private Payers Report Using Data Analytics in Ways Similar to Medicare to Address Fraud**

Organizations representing private payers and vendors of information technology systems reported using data analytics in ways similar to Medicare to detect and mitigate health care fraud. Like Medicare, these selected private payers have not used data analytics to immediately deny claims, but rather to identify anomalous billing patterns to generate leads for provider investigations. They reported using analytics to support actions, such as subjecting providers to prepayment claim reviews and payment suspensions, which can help prevent potentially fraudulent claims from being paid.

The representatives we spoke with reported using the same types of analytic models as Medicare to identify anomalous billing patterns. These include billing spike, peer-to-peer analysis, predictive analytic, and unstructured machine learning models. Neither Medicare nor the selected private payers are currently using generative AI, or AI that can generate novel content, to identify potential fraud. Some of those we spoke with raised concerns about the risks of using such technology, including that leads generated by the approaches may be biased, or that the models may "hallucinate" and generate made up results.

Source: GAO analysis of Centers for Medicare & Medicaid Services information and GAO interviews with representatives of private payers and vendors of information technology systems. | GAO-26-107799

## CMS Monitors Leads from FPS Models and Associated Administrative Actions to Update Models

CMS tracks fraud case leads based on each data analytic model in FPS and the administrative actions that derive from those cases. According to CMS officials, these data are used to assess the effectiveness of individual FPS models and to make decisions about whether models need to be updated or retired. In particular, CMS officials noted that they continually monitor FPS model performance, along with other information about ongoing fraud schemes, to determine whether and how to update the models, as needed. For example, CMS officials told us the models are updated to target additional or different billing codes or services based on billing patterns and fraud trends.

CMS also expects the UPICs to suggest updates to the models in FPS to make them more effective. There is functionality within FPS that allows the UPICs to submit formal update requests. Additionally, UPIC representatives told us that CMS hosts monthly calls with them and CMS's modeling contractor to discuss the effectiveness of specific FPS models and to provide feedback and suggest updates to the models.

## CMS Has Begun to Inform Supplemental Payers of Payment Suspensions

CMS has begun to share information about Medicare provider payment suspensions with supplemental payers. Specifically, the agency provided supplemental payers with a report on providers under payment suspensions in December 2025 and January 2026 to support the supplemental payers' own program integrity efforts.[42] According to CMS officials, the agency plans to provide these reports to supplemental

[42]According to CMS, supplemental payers cannot use a provider's Medicare payment suspension as a standalone reason to deny payments, and they are independently responsible for determining appropriate actions based on their own information and justifications.

payers on a monthly basis and will evaluate whether the reports need to be provided more frequently. This is consistent with the leading practice in the Fraud Risk Framework that calls for agencies to effectively collaborate and share information on fraud risks with external stakeholders. Such information sharing will support supplemental payers' efforts to prevent payments for beneficiary cost-sharing on potentially fraudulent claims.

According to CMS officials, when providers are under payment suspensions, Medicare fully processes their claims as usual, but withholds payments while further investigations are being completed. Because claims for suspended providers are fully processed, they show as approved in the information technology system that is the interface between Medicare and the supplemental payers. Prior to December 2025, CMS generally did not inform supplemental payers of provider payment suspensions.[43] According to CMS, the agency previously did not share payment suspension information with supplemental payers in part because of concerns related to due process and protecting provider privacy.[44]

Representatives of some supplemental payers told us that they paid for Medicare beneficiary cost sharing on potentially fraudulent claims, in part because CMS did not inform supplemental payers of provider payment suspensions.[45] In particular, we found that some supplemental payers had made beneficiary cost-sharing payments to the 15 providers under payment suspension for the urinary catheter scheme, though the total amount of these payments is not known. The amount of the suspended payments to these 15 potentially fraudulent providers in 2023 and 2024 exceeded $4 billion, according to CMS, and the full amount of beneficiary cost sharing potentially would have equaled hundreds of millions of dollars. However, the private payer association and representatives we spoke with stated that private payers may have paid tens of millions of

[43]CMS officials told us that UPICs may have informally shared Medicare payment suspension information with states as part of their role in combatting Medicaid fraud.

[44]CMS officials also told us that the agency needed to determine its authority to share such information with supplemental payers before doing so.

[45]According to CMS, Medigap issuers have an affirmative obligation to pay claims based on the information they receive from CMS pursuant to sections 1882(c)(3)(A) and (B) of the Social Security Act. While this provision only applies to Medigap plans, according to CMS officials, other Medicare supplemental plans generally follow the same procedures established by these authorities.

dollars in aggregate across payers, but none provided exact amounts.[46] Many private supplemental payers had independently identified providers involved in urinary catheter scheme through their own anti-fraud activities and some private supplemental payers withheld payments as a result.[47]

In addition, based on our analysis of state Medicaid data, in 2023 and 2024, state Medicaid agencies made at least $196,000 in beneficiary cost-sharing payments to the 15 providers involved in the urinary catheter scheme during the period in which they were under Medicare payment suspension.[48] Given the federal government's role in financing Medicaid, the $196,000 in payments include both the federal and state shares. Several factors may explain the relatively small amount of Medicaid's supplemental payments to the providers involved in the urinary catheter scheme. For example, providers need to be enrolled in the state's Medicaid program to receive beneficiary cost sharing payments, and officials from one UPIC told us that, in their experience, providers engaged in Medicare fraud often do not enroll in state Medicaid programs.[49]

[46]Not all payers and associations that we spoke with provided estimates to GAO.

[47]Representatives of private payers told us they withheld payments by either putting the providers on prepayment claim review, or by independently gathering evidence supporting possible fraud.

[48]States may contract with private managed care plans to administer state Medicaid services. The $196,000 amount may not include payments made by Medicaid managed care plans for certain states.

[49]In addition, according to CMS officials, UPICs may share payment suspension information with state Medicaid agencies, which can allow states to take action to address potentially fraudulent supplemental claims. Also, depending on state policies, states are not obligated to pay the full beneficiary cost-sharing amount if total payment to the provider would exceed the state's Medicaid rate, which are usually lower than or equal to the Medicare rate. When the state is paying the cost-sharing amount based on a rate below the Medicare rate, it can result in a cost-sharing amount of zero. For example, if the Medicare rate for a Part B service is $100, Medicare would pay $80 and the beneficiary cost-sharing amount is $20. If the state is paying the cost-sharing based on the state's Medicaid rate, and the state's Medicaid rate is less than $80, then the state does not pay anything and the claim is considered paid in full. For more information see MACPAC, *Report to the Congress on Medicaid and CHIP*, "Medicaid Coverage of Premiums and Cost Sharing for Low-Income Medicare Beneficiaries" (Washington, D.C.: Mar. 15, 2013).

## CMS Estimates It Prevented Billions in Potentially Fraudulent Payments from 2022 through 2024

UPIC fraud cases, including those involving the use of FPS, informed CMS administrative actions that CMS estimates prevented billions of potentially fraudulent Medicare payments. For fiscal years 2022 through 2024, CMS reported that UPIC fraud cases prevented a total of $11.9 billion in potentially fraudulent Medicare payments, as shown in table 3.[50] See Appendix III for data on potentially fraudulent payments prevented by year. CMS tracks the role of FPS in administrative actions and the associated potentially fraudulent payments that were prevented.[51] During this period, about 40 percent of UPIC cases involved the use of FPS during the investigation, according to CMS officials.

[50]This amount includes projected amounts of potentially fraudulent payments prevented for certain administrative actions. The projected amounts represent the estimated cost avoidance from having taken the administrative actions. After implementing FPS in 2011, CMS submitted three required annual reports on FPS's implementation to Congress in which the HHS-OIG certified the reported potentially fraudulent payments prevented that were attributed to FPS. CMS also implemented HHS-OIG recommendations to improve the methodology for calculating the amount of potentially fraudulent payments prevented from HHS-OIG, *The Centers for Medicare & Medicaid Services Could Improve Its Processes for Evaluating and Reporting Payment Recovery Savings Associated with the Fraud Prevention System*, A-01-15-00510 (Washington, D.C.: Oct. 23, 2019).

[51]CMS tracks cases as linked to FPS if FPS information is an input to developing the lead for the case, even when FPS information may not materially contribute to investigative activities or ensuing actions. According to officials, CMS does not track the "primary source" of leads that initiate fraud cases because many leads derive from multiple sources.

**Table 3: CMS Administrative Actions and Estimates of Potentially Fraudulent Payments Prevented, Fiscal Years 2022 through 2024**

| | Number of providers or referrals | | Prevented payments (in millions) | |
|---|---|---|---|---|
| **Administrative action** | **Total** | **FPS-linked** | **Total** | **FPS-linked** |
| Prepayment claim review[a] | 1,163[b] | —[c] | $27 | —[c] |
| Automated prepayment denials[a] | 26,819[b] | —[c] | $132 | —[c] |
| Overpayment recoveries | 6,825[b] | 2,482[b] | $652 | $304 |
| Payment suspensions | 1,160 | 423 | $2,579[d] | $1,073[d] |
| Revocations and deactivations | 569 | 164 | $7,962[d] | $505[d] |
| Law enforcement referrals[e] | 709 | 328 | $554[f] | $176[f] |
| **Total** | —[g] | —[g] | **$11,906** | **$2,057** |

Source: GAO analysis of Centers for Medicare & Medicaid Services (CMS) data. | GAO-26-107799

Notes: Data are based on Unified Program Integrity Contractor fraud cases. CMS tracks a case as linked to the Fraud Prevention System (FPS) if FPS information is an input to developing the lead for the case, even when FPS information may not materially contribute to investigative activities or ensuing actions.

[a]Providers who are subject to prepayment claim reviews are required to submit medical records to support their claims before payment will be made, and claims that do not comply with Medicare coverage requirements are denied. If a provider does not submit the requested records in a timely manner, those claims are subject to an automated denial. Automated prepayment denials also include prepayment edits specific to individual providers that automatically deny payments to the provider, such as provider claims for a specific service.

[b]We aggregated data from fiscal years 2022 through 2024 and some individual providers were included in counts in more than one year. Accordingly, the total may include individual providers that were counted more than once.

[c]CMS does not track whether prepayment denials are FPS-linked because of how its fraud management information technology system interacts with Medicare claims data systems.

[d]This is the projected amount of potentially fraudulent payments prevented, which represents the estimated cost avoidance from having taken the administrative actions.

[e]These are case referrals that were accepted by law enforcement. A referral may be for a single provider or a network of providers.

[f]This is an estimated amount in financial judgments that courts may order on behalf of Medicare.

[g]The number of providers subject to administrative actions cannot be totaled as they may vary by action. For example, prepayment reviews are counted based on the number of providers subject to review, while law enforcement referrals are based on the number of referred cases accepted by law enforcement, which may be for a single provider, or a network of providers. Additionally, a single provider may be subject to multiple actions. For example, CMS may both suspend payment to a provider and revoke their enrollment.

Potentially fraudulent payments data may be totaled, as CMS calculations account for potential double counting of providers subject to more than one administrative action. For example, CMS suspended payments to and later revoked the enrollment of a group of 15 providers that allegedly attempted to bill Medicare for more than $4 billion for catheters that were not needed and never provided to Medicare beneficiaries. Some prevented payments associated with this scheme are tracked as prevented payments from payment suspensions and some are tracked as prevented payments from revocations.

Of the estimated $11.9 billion in potentially fraudulent Medicare payments prevented in fiscal years 2022 through 2024, around $7 billion was the result of non-FPS revocations in fiscal year 2024. According to CMS officials, the majority of the $7 billion was primarily associated with providers involved in the urinary catheter scheme and whose Medicare enrollment was revoked.

## Agency Comments

We provided a draft of this report to HHS for review and comment. HHS provided technical comments, which we incorporated as appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees, the Secretary of Health and Human Services, and other interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Leslie Gordon at GordonLV@gao.gov or Seto J. Bagdoyan at BagdoyanS@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely,

//SIGNED//

Leslie V. Gordon
Director, Health Care

//SIGNED//

Seto J. Bagdoyan
Director, Forensic Audits and Investigative Service

# Appendix I: Objectives, Scope, and Methodology

This report (1) describes characteristics of common Medicare fraud schemes; (2) describes the Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services' (CMS) use of data analytics to identify, prevent, and mitigate Medicare fraud; (3) examines the extent to which CMS shares information on payment suspensions with relevant entities; and (4) describes CMS's estimates of the amount of potentially fraudulent payments that it prevented in fiscal years 2022 through 2024.

To describe characteristics of common Medicare fraud schemes, we reviewed HHS and CMS documentation, including annual Medicare program integrity reports to Congress.[1] We also reviewed Department of Justice (DOJ) documentation, including indictments and press releases describing Medicare fraud schemes. We interviewed CMS and HHS Office of Inspector General (HHS-OIG) officials and representatives from all five Unified Program Integrity Contractors (UPIC)—program integrity contractors responsible for identifying and investigating potential Medicare fraud—about common Medicare schemes, how they typically work, the types of Medicare services that are most susceptible to fraud, and CMS efforts to address the schemes. Our information on common Medicare fraud schemes does not cover all possible forms or types of Medicare fraud. In addition, to provide further context on how fraudsters could obtain information needed to commit Medicare fraud, we reviewed "dark web" marketplaces and made two separate purchases of beneficiaries' personally identifiable information, including confidential Medicare beneficiary identifiers (MBI).[2] We compared the MBI data against Medicare enrollment data and confirmed the information was valid.

To describe CMS's use of data analytics to identify, prevent, and mitigate Medicare fraud, we reviewed CMS documentation. This included documentation on data analytic systems used by the agency to identify and track potentially fraudulent Medicare payments, UPIC statements of work and data analytic workplans, and Medicare's program integrity policy manual. We interviewed CMS officials and UPIC representatives to obtain information on how they use data analytics to mitigate fraud. We also

[1]For the purposes of our analysis, a fraud scheme is defined as alleged or adjudicated illegal conduct involving misrepresentation carried out against Medicare using one or more processes, techniques, or systems for profit or other gain.

[2]The "dark web" is a hidden part of the internet that users access using specialized software. We referred information on our purchases to HHS-OIG for possible further investigation.

reviewed CMS's process for assessing the agency's Fraud Prevention System (FPS)—a data analytic system used by CMS and UPICs to identify potential fraud—through a system demonstration by CMS officials, reviewing documentation on agency processes for obtaining UPIC feedback on FPS model performance, and interviews with UPIC representatives.[3]

For additional context on CMS's use of data analytics, we interviewed representatives of five private payers and two organizations representing private payers about their use of data analytics. Our judgmental, non-generalizable selection of the five payers was based on their Medicare Advantage enrollment and marketing of plans in geographic areas of the country identified by CMS officials as having a high prevalence of health care fraud. We also interviewed representatives of three information technology vendors that market data analytic systems. Our judgmental, non-generalizable selection of these vendors was based on a snowball methodology whereby private payers or other information technology vendors we interviewed referred us to additional vendors.

To examine the extent to which CMS shares information on payment suspensions, we interviewed CMS officials on agency processes for sharing information on payment suspensions with supplemental payers. These supplemental payers, including private Medigap plans and state Medicaid agencies, cover certain Medicare beneficiaries' out-of-pocket expenses.[4] As part of our assessment, we also interviewed representatives of private payers and private payer associations and obtained estimates of supplemental payments made to the providers whose payments were suspended for involvement in the urinary catheter scheme. We also analyzed Transformed Medicaid Statistical Information System data on Medicaid payments across all 50 states and the District of Columbia to 15 providers involved in the scheme during the period of their payment suspensions. To assess the reliability of the Medicaid payment data, we reviewed related documentation, and interviewed CMS officials and officials from three state Medicaid agencies. We determined that the data were sufficiently reliable for the purposes of our report. In addition, we evaluated CMS's information sharing against a relevant

[3]Our review focuses on CMS's use of FPS to identify providers engaged in potential fraud. FPS also executes prepayment edits that deny payments for claims that do not comply with Medicare coverage requirements. We did not review FPS's use of prepayment edits.

[4]Medicare beneficiaries may purchase supplemental coverage from private health insurance plans, called Medigap. Medicaid is a joint federal-state program that finances health care for low-income and medically needy individuals.

leading practice for stakeholder collaboration identified in *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).[5] Specifically, this leading practice for implementing anti-fraud activities is for agencies to establish collaborative relationships with relevant external entities, including sharing information on fraud risks.

To describe CMS's estimates of the amount of potentially fraudulent payments that it prevented in fiscal years 2022 through 2024, we obtained and analyzed CMS data for those years on administrative actions taken, and the associated amounts of potentially fraudulent payments that were prevented.[6] We did not independently corroborate CMS's estimates. To assess the reliability of CMS's data, we compared the data to published reports and interviewed agency officials. We determined that the data were sufficiently reliable for the purposes of our report.

We conducted this performance audit from September 2024 to March 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additionally, our related investigative work was conducted in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

[5]See GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

[6]Throughout this report, we use the term "potentially fraudulent payments" to refer to improper payments that were identified through CMS's and the UPICs' anti-fraud activities.

Data from 2024 was the most recent data available at the time of our review, and we also reviewed data from 2022 and 2023 for additional context.

# Appendix II: Medicare Fraud and Accountable Care Organizations

A recent case involving the inappropriate billing of urinary catheters raised questions about how significant amounts of fraud could impact shared savings payments to Medicare accountable care organizations. Accountable care organizations are groups of doctors, hospitals, and other health care providers that work together to coordinate beneficiary care and manage costs in traditional Medicare. These organizations may be eligible to receive shared savings payments based on their care quality and cost savings performance; in certain cases, accountable care organizations may see reduced payments based on their performance.

In 2023 and 2024, a group of 15 providers allegedly attempted to bill Medicare for more than $4 billion for catheters that were not needed and never provided to Medicare beneficiaries, according to the Centers for Medicare & Medicaid Services (CMS). Through early identification of the scheme, CMS implemented payment suspensions that the agency said prevented over 99 percent of the payments from being made.[1] Accountable care organizations raised questions about how the potentially fraudulent billing for the catheters would impact other providers grouped into accountable care organizations with those providers alleged to have fraudulently billed for the catheters.[2] In particular, payments made for the catheters could have lowered accountable care organizations' cost savings performance and accordingly reduced payments to all providers in the organizations.

In response to these concerns, in September 2024, CMS issued a final rule retroactively excluding payments associated with urinary catheters in 2023 from the methodology used to calculate accountable care organization performance payments.[3] In December 2024, CMS issued another final rule that allows the agency to retroactively exclude specific services from performance payment calculations in response to suspect

[1]See Department of Health and Human Services, Centers for Medicare & Medicaid Services, *Urinary Catheter Case Study: CMS' Swift Action Saves Billions,* Sept. 23, 2024.

[2]Accountable care organizations raised such concerns before CMS publicly stated in September 2024 that it had suspended payments on most of the payments associated with the catheter case.

[3]89 Fed. Reg. 79,152 (Sept. 27, 2024) (codified at 42 C.F.R. § 425.670).

billing patterns that would significantly affect the accuracy of the performance payments.[4]

[4]89 Fed. Reg. 97,710 (Dec. 9, 2024) (codified at 42 C.F.R. § 425.672). The rule allows CMS to retroactively exclude payments made for specific services starting with payments made during calendar year 2024. CMS anticipated that any determinations to exclude specific services from performance payment calculations would occur at the beginning of a calendar year and apply to payments from the prior calendar year.

# Appendix III: Administrative Actions and Potentially Fraudulent Payments Prevented by CMS, Fiscal Years 2022 through 2024

Tables 4 and 5 present data from the Department of Health and Human Services' Centers for Medicare & Medicaid Services (CMS) on Unified Program Integrity Contractor administrative actions taken against Medicare providers, and CMS-estimated amounts of potentially fraudulent payments prevented, associated with administrative actions for fiscal years 2022 through 2024.

**Table 4: Number of Providers or Referrals Associated with CMS Administrative Actions, by Year, Fiscal Years 2022 through 2024**

| | 2022 | | 2023 | | 2024 | |
|---|---|---|---|---|---|---|
| **Administrative action** | **Total** | **FPS-linked** | **Total** | **FPS-linked** | **Total** | **FPS-linked** |
| Prepayment claim review denials[a] | 389 | —[b] | 443 | —[b] | 331 | —[b] |
| Automated prepayment denials[a] | 10,756 | —[b] | 8,453 | —[b] | 7,610 | —[b] |
| Overpayment recoveries | 1,971 | 568 | 2460 | 897 | 2,394 | 1,017 |
| Payment suspensions | 451 | 130 | 406 | 156 | 303 | 137 |
| Revocations and deactivations | 185 | 43 | 170 | 41 | 214 | 80 |
| Law enforcement referrals[c] | 250 | 101 | 227 | 112 | 232 | 115 |

Source: GAO analysis of Centers for Medicare & Medicaid Services (CMS) data. | GAO-26-107799

Notes: Data are based on Unified Program Integrity Contractor fraud cases. CMS tracks a case as linked to the Fraud Prevention System (FPS) if FPS information is used as part of developing the lead for the case, even when FPS information may not materially contribute to investigative activities or ensuing actions.

The number of providers subject to administrative actions cannot be totaled as they may vary by action. For example, prepayment reviews are counted based on the number of providers subject to review, while law enforcement referrals are based on the number of referred cases accepted by law enforcement, which may be for a single provider, or a network of providers. Additionally, a single provider may be subject to multiple actions. For example, CMS may both suspend payment to a provider and revoke their enrollment.

[a]Providers who are subject to prepayment claim reviews are required to submit medical records to support their claims before payment will be made, and claims that do not comply with Medicare coverage requirements are denied. If a provider does not submit the requested records in a timely manner, those claims are subject to an automated denial. Automated prepayment denials also include prepayment edits specific to individual providers that automatically deny payments to the provider, such as provider claims for a specific service.

[b]CMS does not track whether prepayment denials are FPS-linked because of how its fraud management information technology system interacts with Medicare claims data systems.

[c]These are case referrals that were accepted by law enforcement. A referral may be for a single provider or a network of providers.

**Table 5: CMS Estimates of Potentially Fraudulent Payments Prevented, by Administrative Action and Year, Fiscal Years 2022 through 2024**

Dollars in millions

| | 2022 | | 2023 | | 2024 | |
|---|---|---|---|---|---|---|
| **Administrative action** | **Total** | **FPS-linked** | **Total** | **FPS-linked** | **Total** | **FPS-linked** |
| Prepayment claim review denials[a] | $7 | —[b] | $11 | —[b] | $8 | —[b] |
| Automated prepayment denials[a] | $25 | —[b] | $39 | —[b] | $68 | —[b] |
| Overpayment recoveries | $116 | $45 | $199 | $65 | $337 | $193 |
| Payment suspensions[c] | $498 | $120 | $1,519 | $639 | $563 | $314 |
| Revocations and deactivations[c] | $351 | $160 | $388 | $136 | $7,222 | $209 |
| Law enforcement referrals[d] | $63 | $38 | $158 | $68 | $333 | $70 |
| **Total[e]** | **$1,060** | **$363** | **$2,314** | **$908** | **$8,530** | **$786** |

Source: GAO analysis of Centers for Medicare & Medicaid Services (CMS) data. | GAO-26-107799

Notes: Data are based on Unified Program Integrity Contractor fraud cases. CMS tracks a case as linked to the Fraud Prevention System (FPS) if FPS information is used as part of developing the lead for the case, even when FPS information may not materially contribute to investigative activities or ensuing actions.

[a]Providers who are subject to prepayment claim reviews are required to submit medical records to support their claims before payment will be made, and claims that do not comply with Medicare coverage requirements are denied. If a provider does not submit the requested records in a timely manner, those claims are subject to an automated denial. Automated prepayment denials also include prepayment edits specific to individual providers that automatically deny payments to the provider, such as provider claims for a specific service.

[b]CMS does not track whether prepayment denials are FPS-linked because of how its fraud management information technology system interacts with Medicare claims data systems.

[c]This is the projected amount of potentially fraudulent payments prevented, which represents the estimated cost avoidance from having taken the administrative actions.

[d]This is based on case referrals (which may be for a single provider or network of providers) that were accepted by law enforcement. The amount is an estimate based on financial judgments that courts may order on behalf of Medicare.

[e]CMS's calculations for the total amount of potentially fraudulent payments prevented do not double count providers subject to more than one administrative action. For example, CMS suspended payments to and later revoked the enrollment of a group of 15 providers that allegedly attempted to bill Medicare for more than $4 billion for catheters that were not needed and never provided to Medicare beneficiaries. Some prevented payments associated with this scheme are tracked as prevented payments from payment suspensions and some are tracked as prevented payments from revocations.

# Appendix IV: GAO Contacts and Staff Acknowledgments

## GAO Contacts

Leslie V. Gordon at GordonLV@gao.gov, or
Seto J. Bagdoyan at BagdoyanS@gao.gov

## Staff Acknowledgments

In addition to the contacts named above, Dean Campbell and Corissa Kiyan-Fukumoto (Assistant Directors), Michael Erhardt (Analyst-in-Charge), Jennie Apter, Robert Bastian, Julianne Flowers, Joy Grossman, Melissa Hart, Madison Herin, Ariel Landa-Seiersen, James Murphy, Patricia Powell, Jennifer Rudisill, Roxanna Sun, and Jeff Tamburello made key contributions to this report.

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

## Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

## Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

## Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

## General Inquiries

https://www.gao.gov/about/contact-us