Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

CMS AND ITS CONTRACTORS DID NOT USE COMPREHENSIVE ERROR RATE TESTING PROGRAM DATA TO IDENTIFY AND FOCUS ON ERROR-PRONE PROVIDERS

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Christi A. Grimm
Principal
Deputy Inspector General

January 2021
A-05-17-00023

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These audits help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that

OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief
Date: January 2021
Report No. A-05-17-00023

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

CMS and Its Contractors Did Not Use Comprehensive Error Rate Testing Program Data To Identify and Focus on Error-Prone Providers

Why OIG Did This Audit

Public law requires the heads of Federal agencies to annually review programs that they administer to identify and develop actions to reduce improper payments.

The Centers for Medicare & Medicaid Services (CMS) administers the Comprehensive Error Rate Testing (CERT) program to measure improper Medicare fee-for-service payments to providers.

Previous OIG reports recommended using CERT data to identify and focus on providers that were prone to having errors.

Our objective was to determine whether CMS and its contractors used CERT program data to identify and focus on error-prone providers.

How OIG Did This Audit

We reviewed the steps CMS and its contractors took to reduce the improper payment rates for the reporting years 2014 through 2017, which included reviewing and analyzing the CERT program data to identify error-prone providers for fiscal years 2014 through 2017.

What OIG Found

CMS and its contractors did not use CERT data to identify and focus on error-prone providers for review and corrective action. Using CERT data, we identified 100 error-prone providers from 2014 through 2017. Of the $5.8 million reviewed by CERT, $3.5 million was incorrect, which is an improper payment rate of 60.7 percent. We determined that during the same period, Medicare made $19.1 billion in FFS payments to these 100 error-prone providers.

The term "error-prone provider" is an OIG-created term to refer to a list of providers identified as having higher rate of errors in the CERT sample data. When used to describe OIG analysis of CERT data from 2014 through 2017, the term refers to providers that had at least one error in each of the 4 CERT years analyzed, an error rate of higher than 25 percent in each of the 4 CERT years analyzed, and a total error amount of at least $2,500. An error-prone provider is statistically more likely to submit an improper claim than the average provider.

What OIG Recommends and Auditee Comments

We recommend that CMS: (1) review the list of 100 error-prone providers identified in this audit and take specific action as appropriate, such as prior authorization, prepayment reviews, and postpayment reviews, and (2) use annual CERT data to identify individual providers that have an increased risk of receiving improper payments and apply additional program integrity tools to these providers.

In written comments on our draft report, CMS did not concur with our recommendations. CMS disagreed with our methodology for identifying error-prone providers and suppliers. Additionally, CMS stated that it previously attempted to use CERT data to identify error-prone providers and suppliers but found that CERT data was ineffective for this purpose and discontinued the practice.

After reviewing CMS's comments, we maintain that our findings and recommendations remain valid. We maintain that CMS can improve its ability to detect these types of providers by using the provider-level CERT data along with its existing oversight efforts.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Improper Payments Information Act of 2002 (IPIA), as amended by the Improper Payments Elimination and Recovery Act of 2010 (IPERA) and the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), requires the heads of Federal agencies to annually review programs that they administer to identify and develop actions to reduce improper payments.

The Centers for Medicare & Medicaid Services (CMS) administers the Comprehensive Error Rate Testing (CERT) program to measure improper Medicare fee-for-service (FFS) payments to providers. In 2010, the Office of Inspector General (OIG) reported[1] that CMS and its contractors did not use CERT data to identify and focus on providers that are prone to having errors on their FFS claims (error-prone providers). The report recommended that CMS implement corrective actions, including using available CERT data to identify error-prone providers and sharing this information with contractors so that they can monitor the providers and take appropriate actions to reduce claim errors.

We conducted this audit to determine whether CMS and its contractors used CERT program data to identify and focus on error-prone providers.[2]

OBJECTIVE

Our objective was to determine whether CMS and its contractors used CERT program data to identify and focus on error-prone providers.

BACKGROUND

Medicare Program

Medicare Parts A and B services are provided under the FFS program. Medicare Part A provides inpatient hospital insurance benefits and coverage of extended care services for patients after hospital discharge, and Medicare Part B provides supplementary medical insurance for medical and other health services, including coverage of hospital outpatient services. CMS administers the Medicare program and contracts with Medicare administrative contractors (MACs) to

[1] *Centers for Medicare & Medicaid Services' Use of Medicare Fee-for-Service Error Rate Data To Identify and Focus on Error-Prone Providers* (A-05-08-00080), issued October 7, 2010.

[2] The term "error-prone provider" is an OIG-created term to refer to a list of providers identified as having higher rate of errors in the CERT sample data. When used to describe OIG analysis of CERT data from 2014 through 2017, the term refers to providers that had at least one error in each of the 4 CERT years analyzed, an error rate of higher than 25 percent in each of the 4 CERT years analyzed, and a total error amount of at least $2,500.

process and pay claims submitted by hospitals. CMS made Medicare FFS payments totaling $381 billion in fiscal year (FY) 2017 and $389 billion in FY 2018.

Medicare Contractors

CMS uses contractors to help administer the Medicare program. Among other things, the contractors process FFS claims for payment, enroll providers in the Medicare program, and educate providers about Medicare billing requirements. A detailed list of contractors discussed in this report can be found in Appendix B.

Comprehensive Error Rate Testing Program

Through the CERT program,[3] CMS calculates the FFS improper payment rate.[4] The CERT program is designed to comply with the Payment Integrity Information Act of 2019 (PIIA).[5]

CMS uses a statistical contractor and a medical review contractor to measure the CERT program's improper payment rate. The CERT statistical contractor develops the statistical sample for the CERT program, and the CERT medical review contractor sends a letter to selected providers requesting medical documentation for the claims. The medical review contractor then reviews the medical record documentation to determine whether the claims were paid properly under Medicare coverage, coding, and billing rules. The CERT statistical contractor uses the determinations to estimate the rate of improper payments in Medicare Parts A and B. The claims and medical review determinations made by the independent medical review contractor are known as CERT data. The CERT statistical contractor maintains a database with the most current CERT data.

CMS reported that the estimates of improper FFS payments increased from $28.8 billion in FY 2011 to $31.6 billion in FY 2018. The improper payment amounts peaked at $45.8 billion in 2014. (See Figure 1 on the next page.)

[3] CERT program details and reports can be found at www.cms.gov/cert. Accessed on June 9, 2020.

[4] The improper payment rate is not a "fraud rate"; rather, it is a measurement of payments that did not meet Medicare requirements. Not all payments that fail to meet Medicare requirements constitute fraud.

[5] PIIA was passed into law on March 2, 2020 (after our audit period) to improve efforts to identify and reduce Governmentwide improper payments. PIIA repeals and replaces IPIA, IPERA, and IPERIA. The current CERT program is designed to comply with the requirements of PIIA.

Figure 1: CERT-Reported Improper Payment Rates and Amounts (in billions of dollars)

	Total FFS Payments	Total Improper Payments	Improper Payment Rate
2011	$336.4	$28.8	8.6%
2012	349.7	29.6	8.5%
2013	357.4	36.0	10.1%
2014	360.2	45.8	12.7%
2015	358.3	43.3	12.1%
2016	373.7	41.1	11.0%
2017	380.8	36.2	9.5%
2018	389.3	31.6	8.1%

CMS Medicare Integrity Initiatives

CMS's Medicare integrity initiatives help prevent improper payments and encourage providers to comply with the rules. These initiatives include prepayment and postpayment claim review, the provision of educational information, and the Targeted Probe and Educate (TPE) program.

Prepayment and Postpayment Claim Review

Medicare conducts two types of claim reviews: prepayment and postpayment. A prepayment review occurs when a MAC makes a payment determination before a claim payment has been made. A postpayment review occurs when a reviewer makes a payment determination after a claim has been paid. In interviews with CMS and its contractors,[6] we identified some examples of prepayment and postpayment reviews.

CMS implemented a 100-percent prepayment review demonstration for all HHA claims billed in Illinois from August 2016 through March 2017. CMS reviewed claims prior to payment to determine whether the claims met Medicare requirements.

CMS uses a supplemental medical review contractor (SMRC) to perform medical review on a postpayment basis for skilled nursing facility and inpatient rehabilitation facility services nationwide. The SMRC shares the results of the postpayment review with MACs, who then adjust claims and demand repayment for services that did not meet Medicare requirements.

[6] We conducted interviews with CMS, the CERT medical review and statistical contractor, seven MACS, and seven other types of contractors listed in Appendix B as part of our fieldwork.

Educational Information

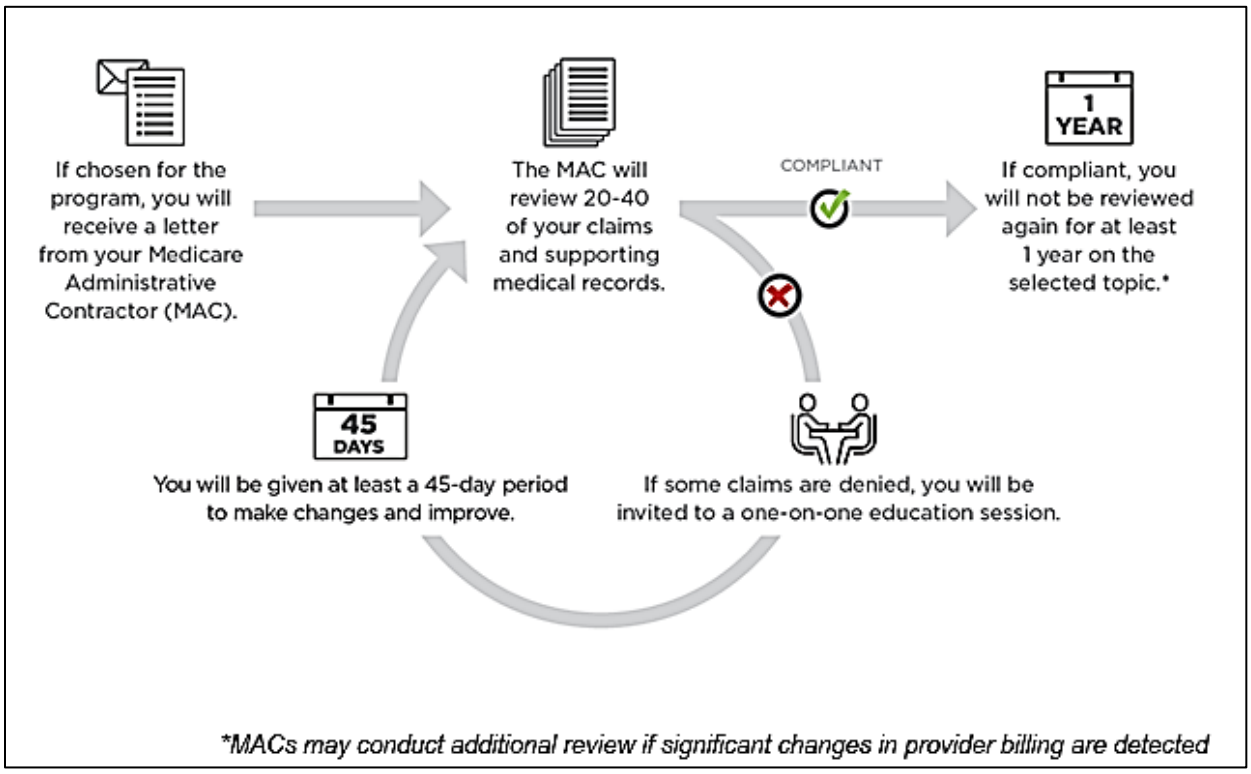
CMS provides articles, coding instructions, and coverage determinations[7] to educate providers about how to correctly submit claims and under what circumstances specified services will be considered reasonable and necessary.

When a claim is denied as part of a postpayment review, the MACs provide detailed letters to providers with information about what was incorrect in the original billing of a claim. The letters are used to educate providers on what specifically was wrong with a submitted claim.

Targeted Probe and Educate Program

In the TPE program, CMS provides one-on-one education to providers with high denial rates or unusual billing practices to help those providers reduce claim errors and denials. Additional details on how the TPE program works are shown in Figure 2.

Figure 2: CMS Targeted Probe and Educate Program—How Does It Work?[8]



[7] Medicare coverage determinations can be found online at https://www.cms.gov/medicare-coverage-database/. Accessed on June 9, 2020.

[8] Figure 2 is a CMS graphic, which is available online at https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Medical-Review/Targeted-Probe-and-EducateTPE.html. Accessed on June 9, 2020.

Medicare Integrity Challenge

One of the top management and performance challenges facing the Department of Health and Human Services (HHS) is ensuring the financial integrity of HHS programs, including Medicare. To address this priority, OIG attempts to identify and recommend methods to minimize inappropriate payments; hold providers accountable for fraud, waste, and abuse within the program; identify ways to close exploited loopholes; and examine payment and pricing methods to ensure that Medicare, its beneficiaries, and taxpayers realize value for program expenditures.

Previous Office of Inspector General Audits

In the 2010 report previously discussed, OIG found that CMS and its contractors did not use historical CERT data to identify and focus on error-prone providers. Using the reported CERT data, OIG identified 740 providers that accounted for a significant portion of the total actual improper payments. The audit found that CERT data were not shared with some contractors. We recommended that CMS use available error-rate data to identify error-prone providers, require error-prone providers to identify the root causes of claim errors and develop and implement corrective action plans, monitor provider-specific corrective action plans, and share error-rate data with its contractors to assist in identifying improper payments. In response to our recommendations, CMS published a list of error-prone providers that was distributed to the contractors.

In 2019, OIG found that focusing on high-risk home health agencies (HHAs) identified using CERT data could provide CMS with opportunities to reduce the improper payments and the overall HHA error rate.[9] The report identified 87 high-risk HHA providers that had an average improper payment rate of 78 percent. Using Medicare program data, we determined that Medicare made $4 billion in FFS payments to these 87 high-risk HHA providers from 2014 through 2017.

HOW WE CONDUCTED THIS AUDIT

We reviewed the steps CMS and its contractors took to reduce the improper payment rates for the reporting years 2014 through 2017. The review included analyzing CERT data to identify error-prone providers for FYs 2014 through 2017.[10] For additional methodology information, see Appendix A.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

[9] *The Centers for Medicare & Medicaid Services Could Use Comprehensive Error Rate Testing Data To Identify High-Risk Home Health Agencies* (A-05-17-00035), issued September 5, 2019.

[10] 2017 was the most recent CERT data available at the time we conducted our analysis.

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.

FINDING

CMS and its contractors did not use CERT data to identify and focus on error-prone providers for review and corrective action. In response to our recommendations in a prior audit report, CMS provided a list of error-prone providers to the MACs; however, in interviews with MAC officials, we found that the list was not useful because CMS did not provide instructions on how to use it. During our current audit, CMS stopped providing the list of error-prone providers to the contractors.[11]

Using CERT data, we identified 100 error-prone providers that received $19.1 billion in Medicare FFS payments from 2014 through 2017. These providers received $3.5 million in overpayments (of $5.8 million reviewed by CERT), which represents a 60.7-percent error rate.[12] This error rate is significantly higher than the national average of 11.3 percent for all Medicare providers over the same period.

An error-prone provider is statistically more likely to submit an improper claim than the average provider.

CMS DID NOT USE COMPREHENSIVE ERROR RATE TESTING PROGRAM DATA TO IDENTIFY AND FOCUS ON ERROR-PRONE PROVIDERS

CMS did not use CERT data to identify and focus on error-prone providers. Although CMS provided contractors with a list of error-prone providers that it identified based on CERT data, CMS did not instruct its contractors on how to use the list. Most contractor officials we interviewed stated that they generally did not use the list of error-prone providers in their program integrity activities because the list did not provide details that allowed them to readily determine which providers fell within their jurisdiction. During our audit, CMS stopped providing the list of error-prone providers to the contractors.

Although CMS and its contractors did not use historical CERT data to identify and focus on error-prone providers, CMS targeted its efforts to reduce the improper payment error rate toward certain types of services. Specifically, CMS identified three types of service areas (home

[11] CMS stopped providing the error-prone provider list to contractors because of concerns that CERT data may not be useful for identifying error-prone providers because these data are designed to generate a national error rate.

[12] The error percentage is calculated by using the improper payment dollar amount divided by the total dollar amount reviewed ($3,500,600 in improper payments divided by $5,766,550 in total payments reviewed).

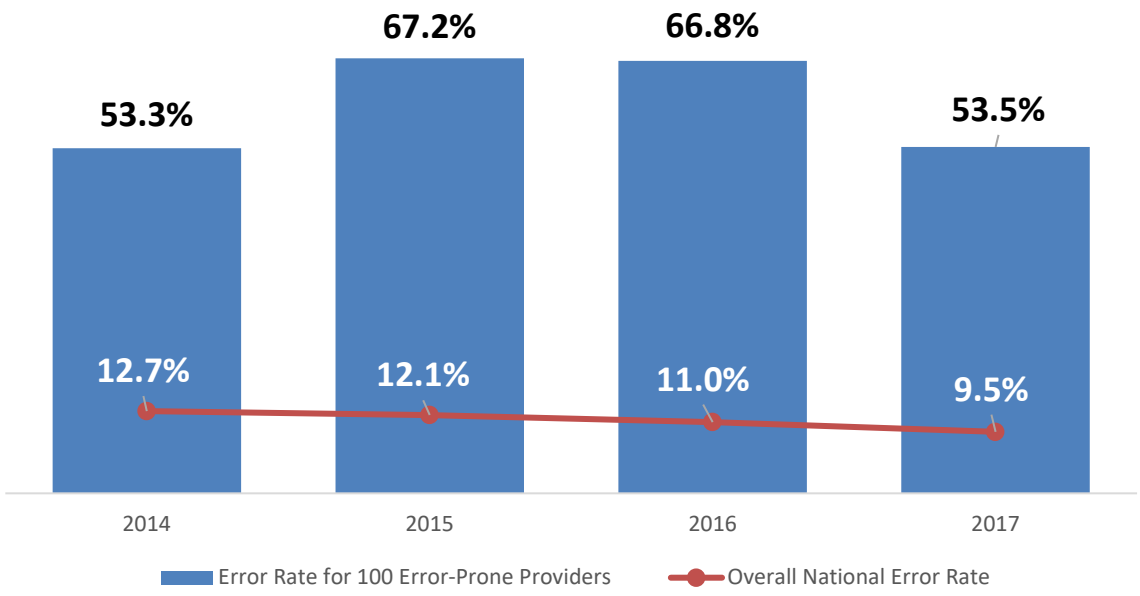
health, inpatient rehabilitation, and skilled nursing)[13] for which corrective actions would have the biggest impact on the overall error rate. Using this or similar analysis can have significant value as part of a multifaceted approach to program integrity.

Medicare Paid 100 Error-Prone Providers $19.1 Billion in Fee-for-Service Payments From 2014 Through 2017

Using CERT data from 2014 through 2017, we selected 100 error-prone providers.[14] Of the $5.8 million reviewed by CERT for these providers, $3.5 million was incorrect, which is an improper payment rate of more than 60.7 percent. We determined that during the same period, Medicare made $19.1 billion in FFS payments to these 100 error-prone providers.

In FYs 2014 through 2017, the annual error rate for these 100 error-prone providers was significantly higher than the overall national error rate, as shown in Figure 3.

Figure 3: Improper Payment Rates for the 100 Error-Prone Providers Compared With All Providers Nationwide

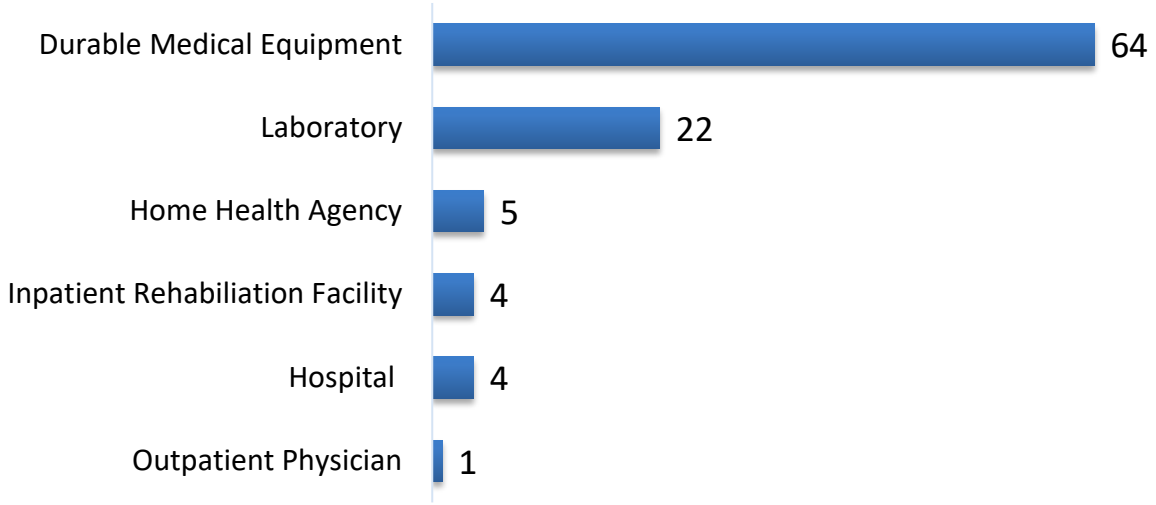


[13] In the 2017 CMS Agency Financial Report, CMS identified three service areas that were major contributing factors to the improper payment rate.

[14] For the purpose of our analysis, error-prone providers were defined as providers that had at least one error in each CERT year, an error rate of higher than 25 percent in each of the 4 CERT years analyzed, and a total error amount of at least $2,500. The top 100 error-prone providers were identified by sorting the total dollar amount in error over the 4-year period from largest to smallest.

The 100 error-prone providers fell into 6 provider types. Of the 100 error-prone providers, 91 fell outside of CMS's identified service areas of home health, inpatient rehabilitation, and skilled nursing. We break down the six provider types in Figure 4.

Figure 4: 100 Error-Prone Providers by Provider Type



Additionally, we found that the top 10 error-prone providers by dollar amount in error received more than $3.2 billion in FFS payments from 2014 through 2017. These top 10 providers accounted for $2.4 million in improper payments (of $4.0 million reviewed by CERT), as shown in Figure 5.

Figure 5: Top 10 Error-Prone Providers Identified in CERT Data

FYs 2014 Through 2017					
Provider	**Provider Type***	**Payments Reviewed**	**Improper Payments**	**Improper Payment Rate**	**FFS Payments**
1	Hospital	$1,323,478	$675,375	51.0%	$24,141,834
2	IRF	528,818	465,866	88.1%	464,442,073
3	Hospital	659,081	303,856	46.1%	330,934,386
4	IRF	217,027	192,882	88.9%	152,484,458
5	Hospital	499,984	183,153	36.6%	149,497,428
6	DME	360,484	169,428	47.0%	1,382,730,676
7	IRF	125,206	125,206	100.0%	108,291,752
8	IRF	91,303	91,303	100.0%	92,473,128
9	HHA	128,866	90,324	70.1%	6,871,285
10	LAB	79,086	72,913	92.2%	504,590,388
Total		**$4,013,333**	**$2,370,306**	**59.06%**	**$3,216,457,408**

***Inpatient Rehabilitation Facility (IRF), Durable Medical Equipment (DME), Home Health Agency (HHA), and Laboratory (LAB).**

For some providers, the evidence in CERT of systematic compliance issues is unequivocal. For example, one provider had an average sample error rate of 92 percent. The provider's sample error rate was consistently high, starting at 79 percent in 2014, and it did not drop below 90 percent for the remaining 3 years of our review. These results were identified across over 3,000 claims from the provider that were included in the CERT sample. Given the consistency and magnitude of the errors along with the number of claims sampled, the CERT data provides substantial evidence that a large majority of the $500 million in FFS payments this provider received during our audit period were improper.

CONCLUSION

We believe that the results of our audit demonstrate that historic CERT data can be used to identify error-prone providers that may be at risk for significant Medicare overpayments. An error-prone provider is statistically more likely to submit an improper claim than the average provider. Using CERT data, we identified 100 error-prone providers from 2014 through 2017. Of the $5.8 million reviewed by CERT, $3.5 million was incorrect, which is an improper payment rate of 60.7 percent. We determined that during the same period, Medicare made $19.1 billion in FFS payments to these 100 error-prone providers. Using this or similar analysis can have significant value as part of a multifaceted approach to program integrity.

RECOMMENDATIONS

We recommend that the Centers for Medicare & Medicaid Services:

- review the list of 100 error-prone providers identified in this audit and take specific action as appropriate, such as prior authorization, prepayment reviews, and postpayment reviews, and

- use annual CERT data to identify individual providers that have an increased risk of receiving improper payments and apply additional program integrity tools to these providers.

CMS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, CMS did not concur with our recommendations. CMS disagreed with our methodology for identifying error-prone providers and suppliers, stated that it previously attempted to use CERT data to identify error-prone providers but found that CERT data were ineffective for this purpose, and believes that the methods CMS currently uses to identify error-prone providers are methodologically superior and more statistically supportable. CMS's comments appear in their entirety as Appendix C.

After reviewing CMS's comments, we maintain that our findings and recommendations are valid. We maintain that CMS can improve its ability to identify error-prone providers by using the provider-level CERT data along with its existing oversight efforts.

CMS COMMENTS

CMS stated that the CERT sampling methodology is designed to meet the Medicare FFS program precision requirement and that the provider- and supplier-level improper payment rates do not have similar precision requirements. CMS believes the OIG methodology is misleading and would be ineffective. In addition, CMS does not believe it is appropriate to use data from the same time period to compare an error-prone provider with the average provider and does not believe our statement that "an error-prone provider is statistically more likely to submit an improper claim than the average provider" is valid.

CMS stated that it previously attempted to use CERT data to identify error-prone providers and suppliers but found that CERT data were ineffective for this purpose and discontinued the practice.

Additionally, CMS said that analysis of CERT program data is only one of many methods that CMS uses to ensure the integrity of the Medicare program. CMS believes that efforts should be focused on those risk areas and associated error-prone providers and suppliers identified through the VCC's [Vulnerability Collaboration Council's] risk-based approach.

OFFICE OF INSPECTOR GENERAL RESPONSE

After reviewing CMS's comments, we disagree with CMS that our method for identifying error-prone providers is misleading and ineffective. We maintain that our findings and recommendations are valid, and that our methodology is sound and can be effective in identifying areas of potential risk, including error-prone providers. Although the CERT program is not designed to identify potential problems at the provider level, we found that analyzing the large volume of claims, especially when aggregated over multiple years, can identify providers that have substantial billing issues. For example, one provider described in this report had a 92-percent error rate across over 3,000 claims that the provider submitted and that were subsequently reviewed by the CERT program. Furthermore, we performed simulation testing to confirm that the providers that we identified are statistically more likely to submit an improper claim than the average provider.

We acknowledge that, in response to our 2012 report, CMS attempted to use CERT data to create a list of error-prone providers. Most contractor officials we interviewed stated that they generally did not use the list of error-prone providers in their program integrity activities because the list did not provide details that allowed them to readily determine which providers fell within their jurisdiction. Contractor officials stated they were not provided with specific instructions or guidance about how to use the list of error-prone providers.

OIG recognizes that CMS uses a variety of program integrity tools to reduce improper payments. We are not suggesting that it discontinue use of these tools. Rather, we believe that our analysis and the analysis done in our 2012 report demonstrate the value of using the

provider-level CERT data along with its existing oversight efforts. The Federal Government makes a significant investment each year in the CERT program to measure improper payments that Medicare makes to providers. We believe that using these data to target error-prone providers will increase the Government's return on the investment made in the CERT program, enhance CMS's ongoing efforts to reduce improper payments, and help protect the integrity of the Medicare Trust Funds.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed the corrective actions CMS has taken to reduce improper payments for reporting years 2014 through 2017. We analyzed claim data from the CERT program for FYs 2014 through 2017. Each claim contained information about the certifying physician, beneficiary, provider, enrollment date, discharge date, and diagnosis codes.

We did not evaluate the internal controls of the CERT program because it was not within the scope of this audit.

We conducted our audit from July 2017 through June 2020, which included visits to CMS in Baltimore, Maryland, and its contractors in various locations.

METHODOLOGY

To accomplish our objective, we:

- reviewed Federal requirements for developing and reporting FFS error rates and estimated improper payments;
- reviewed HHS Agency Financial Reports from 2014 through 2017;
- reviewed Federal program integrity manuals;
- interviewed CMS officials who are involved in the CERT program;
- interviewed officials at the MACs, Recovery Audit Contractors (RACs), Zone Program Integrity Contractors, Unified Program Integrity Contractors, SMRC, and CERT statistical and medical review contractors;
- reviewed CERT program data from FYs 2014 through 2017;
- reviewed CMS's and the Medicare payment contractors' annual Improper Payment Reduction Strategy plans from 2014 through 2017; and
- discussed our findings with CMS officials.

We conducted this performance audit 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.

APPENDIX B: MEDICARE CONTRACTORS

MEDICARE ADMINISTRATIVE CONTRACTORS

MACs are private health care insurers that have been awarded a contract from CMS to process claims, pay providers, review claims, and educate providers on how to submit accurate claims that meet Medicare guidelines. MACs have Provider Outreach and Education units and Provider Contact Centers to assist providers in understanding and complying with Medicare's processes, policies, and billing procedures. MACs also work with CMS's other review contractors (described below) to notify providers of overpayments and underpayments and are authorized to correct improper payments through claim adjustment and other recoupment measures.

COMPREHENSIVE ERROR RATE TESTING PROGRAM MEDICAL REVIEW CONTRACTOR

The CERT medical review contractor is independent of MACs and determines which claims are paid properly under Medicare coverage, coding, and billing rules. This contractor also maintains the CERT provider website, CERT claim status website, and CERT management website.

COMPREHENSIVE ERROR RATE TESTING PROGRAM STATISTICAL CONTRACTOR

The CERT statistical contractor develops the statistical sample for the CERT program and uses errors identified by the independent medical review contractors to estimate the rate of improper payments in Medicare Part A and Part B. The CERT statistical contractor maintains a website that allows other contractors with direct access to the most current CERT data.

RECOVERY AUDIT CONTRACTORS

RACs are paid on a contingency basis to identify improper payments for Part A and Part B claims. The RAC program went nationwide in 2010 and has recovered billions in identified overpayments.

SUPPLEMENTAL MEDICAL REVIEW CONTRACTORS

SMRCs perform reviews focused on lowering the improper payment rate and increasing efficiencies of the medical review functions of the Medicare and Medicaid programs. SMRC reviews may focus on issues identified by CMS internal data analytics, the CERT program, professional organizations, or other Federal agencies (e.g., OIG and the Government Accountability Office).

ZONE PROGRAM INTEGRITY CONTRACTORS AND UNIFIED PROGRAM INTEGRITY CONTRACTORS

Zone Program Integrity Contractors and Unified Program Integrity Contractors investigate instances of suspected fraud, waste, and abuse in Medicare and Medicaid and sometimes identify improper payments that are then recouped by MACs.

APPENDIX C: AUDITEE COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: November 23, 2020

TO: Christi A. Grimm
Principal Deputy Inspector General

FROM: Seema Verma
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: CMS and Its Contractors Did Not Use Comprehensive Error Rate Testing Program Data To Identify and Focus on Error-Prone Providers, A-05-17-00023

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft report. CMS is committed to identifying error-prone providers and suppliers and reducing improper payments in Medicare Fee-for-Service (FFS). As a result of CMS's sustained efforts in preventing and reducing improper payments in Medicare FFS, the improper payment rate decreased from 11.00 percent in Fiscal Year (FY) 2016 to 6.27 percent in FY 2020.

In this report, OIG attempted to identify error-prone providers and suppliers through Comprehensive Error Rate Testing (CERT) data. OIG examined CERT data for providers from FY 2014 through 2017 and identified providers that had at least one error in each of the four CERT years analyzed, an error rate of higher than 25 percent in each of the four CERT years analyzed, and a total error amount of at least $2,500. OIG then labeled these providers and suppliers as "error-prone providers."

CMS does not believe the OIG methodology for identifying error-prone providers and suppliers is valid. The CERT program calculates the improper payment rate for the entire Medicare FFS program by evaluating a statistically valid stratified random sample of claims to determine if they were paid properly under Medicare coverage, coding, and billing rules. The CERT sampling methodology meets the Medicare FFS program precision requirements as required by law and implemented by the Office of Management and Budget A-123, Appendix C.[1] The provider and supplier level improper payment rates do not have similar precision requirements. Also, relying solely on CERT claims to identify error-prone providers and suppliers artificially restricts the universe of providers and suppliers being scrutinized. In FY 2017, CERT reviewed only about 50,000 of the over 1.2 billion Medicare FFS claims, or only about 0.0041 percent of all Medicare FFS claims. That rate represents the normal CERT sampling methodology, and, as noted above, is performed via a valid stratified random sample.

CMS previously attempted to use CERT data to identify error-prone providers and suppliers, but found that CERT data was ineffective for this purpose and discontinued the practice.

[1] The Payment Integrity Information Act of 2019. P.L. 116-117.

Specifically, in response to previous OIG recommendations,[2] from 2013 to 2017 CMS provided the Medicare Administrative Contractors (MACs) analyses of error-prone providers and suppliers identified through CERT data. However, the improper payment measurement guidance does not have provider and supplier level precision requirements, and, because MACs, based on separate work, had more accurate data on providers and suppliers in their jurisdictions, CMS found the practice ineffective and discontinued it. In fact, all Medicare review contractors (MACs, Recovery Audit Contractors, the Supplemental Medical Review Contractor and Unified Program Integrity Contractors) are constantly evaluating the current billing patterns of the providers and suppliers in their jurisdictions with their own data analysis tools. These contractors are not constrained by reporting period windows like CERT and can run data analysis on current claims.

In addition to not agreeing that the OIG methodology for identifying error-prone providers and suppliers is valid, CMS also does not believe that the OIG's methodology for their statement that "an error-prone provider is statistically more likely to submit an improper claim than the average provider" is valid. The OIG used CERT data from FY 2014 through 2017 to identify providers with higher error rates during those years. It is not appropriate to use data from the same time period to compare with the average provider, since these "error-prone providers" were specifically selected for having higher rates of errors in those years.

Importantly, when combined with other sources of information available to CMS and its MACs, CMS does use the CERT program data to address improper payments in Medicare FFS through various corrective actions, such as the Targeted Probe and Educate process. This targeted approach allows MACs to focus on specific providers and suppliers within a service type, rather than all providers and suppliers billing the service. This eliminates the burden to providers and suppliers who, based on data analysis, are already submitting claims that comply with Medicare policy.

CMS is committed to identifying error-prone providers and suppliers and reducing improper payments and currently identifies error-prone providers and suppliers through a variety of methods. CMS utilizes a centralized vulnerability management process to identify, prioritize, track, and mitigate vulnerabilities that affect the integrity of federal health programs. The centralized component of this process, known as the Vulnerability Collaboration Council (VCC), is comprised of CMS leadership and subject matter experts who work collaboratively to identify vulnerabilities that lead to improper payments and develop comprehensive risk strategies to mitigate these vulnerabilities. CMS aligned the VCC's risk-based approach with GAO's fraud risk framework (GAO-15-593SP). By aligning with the GAO framework, CMS standardized the vulnerability management process by focusing on the identification and mitigation of key risk factors through the design and implementation of specific mitigation activities that are regularly evaluated and adapted to adjust to changing circumstances. One such mitigation activity that the VCC is exploring is the development of data analytic methods to identify providers and suppliers that may be more prone to improper payments and to refer these providers and suppliers for additional interventions, including medical review by the MACs and other review contractors. CMS is also using the Fraud Prevention System to identify, at the time of claim submission, when mistakes or intentional behavior may lead to improper payments or indicate fraud.

[2] Centers for Medicare & Medicaid Services' Use of Medicare Fee-For-Service Error Rate Data to Identify and Focus on Error-Prone Providers (A-05-08-00080), Department of Health and Human Services, Office of Inspector General, October 2010, https://oig.hhs.gov/oas/reports/region5/50800080.pdf.

While we appreciate OIG's efforts on this issue and are open to improvements in our program, we maintain that the OIG's suggested methodology to identify "error-prone providers" is misleading and would be ineffective. By contrast, we believe the methods CMS currently uses to ensure the integrity of the Medicare program and identify error-prone providers and suppliers are methodologically superior to, and more statistically supportable than, the OIG's recommendation and, critically, are reliable and effective. We will continue to work with OIG on ways to identify and reduce improper payments.

OIG's recommendations and CMS' responses are below.

OIG Recommendation

The Centers for Medicare & Medicaid Services should review the list of 100 error-prone providers identified by this audit and take specific action as appropriate, such as prior authorization, prepayment reviews, and postpayment reviews.

CMS Response

CMS does not concur with this recommendation. As explained above, the improper payment measurement guidance does not have provider and supplier level precision requirements. CMS previously attempted to use CERT data to identify error-prone providers and suppliers, but found that CERT data was ineffective for this purpose and discontinued the practice. Analysis of CERT program data is only one of many methods that CMS uses to ensure the integrity of the Medicare program. CMS believes that efforts should be focused on those risk areas and associated error-prone providers and suppliers identified through the VCC's risk-based approach.

OIG Recommendation

The Centers for Medicare & Medicaid Services should use annual CERT data to identify individual providers that pose an increased risk of receiving improper payments and apply additional program integrity tools to these providers.

CMS Response

CMS does not concur with this recommendation. As explained above, the improper payment measurement guidance does not have provider and supplier level precision requirements. CMS previously attempted to use CERT data to identify error-prone providers and suppliers, but found that CERT data was ineffective for this purpose and discontinued the practice. Analysis of CERT program data is only one of many methods that CMS uses to ensure the integrity of the Medicare program.

CMS thanks OIG for their efforts on this issue and looks forward to working with OIG on this and other issues in the future.