# Department of Health and Human Services

## OFFICE OF INSPECTOR GENERAL

# CMS AND ITS CONTRACTORS HAVE ADOPTED FEW PROGRAM INTEGRITY PRACTICES TO ADDRESS VULNERABILITIES IN EHRS

**Daniel R. Levinson**
**Inspector General**

**January 2014**
**OEI-01-11-00571**

## EXECUTIVE SUMMARY: CMS AND ITS CONTRACTORS HAVE ADOPTED FEW PROGRAM INTEGRITY PRACTICES TO ADDRESS VULNERABILITIES IN EHRS
## OEI-01-11-00571


### WHY WE DID THIS STUDY
Electronic health records (EHRs) replace traditional paper medical records with computerized recordkeeping to document and store patient health information. Experts in health information technology caution that EHR technology can make it easier to commit fraud. For example, certain EHR technology features may be used to mask true authorship of the medical record and distort information to inflate health care claims. The transition from paper records to EHRs may present new vulnerabilities and require the Centers for Medicare & Medicaid Services (CMS) and its contractors to adjust their techniques for identifying improper payments and investigating fraud.

### HOW WE DID THIS STUDY
We sent an online questionnaire to CMS administrative and program integrity contractors that use EHRs to pay claims, identify improper Medicare payments, and investigate fraud. We also reviewed guidance documents and policies on EHRs and fraud vulnerabilities that CMS and its contractors released for health care providers. Lastly, we reviewed documents on EHRs and Medicare claims that CMS provided to its contractors.

### WHAT WE FOUND
CMS and its contractors had adopted few program integrity practices specific to EHRs. Specifically, few contractors were reviewing EHRs differently from paper medical records. In addition, not all contractors reported being able to determine whether a provider had copied language or overdocumented in a medical record. Finally, CMS had provided limited guidance to Medicare contractors on EHR fraud vulnerabilities.

### WHAT WE RECOMMEND
Although EHR technology may make it easier to perpetrate fraud, CMS and its contractors have not adjusted their practices for identifying and investigating fraud in EHRs. Our report made two recommendations. First, CMS should provide guidance to its contractors on detecting fraud associated with EHRs. CMS could work with contractors to identify best practices and develop guidance and tools for detecting fraud associated with EHRs. Second, CMS should direct its contractors to use providers' audit logs. Audit log data distinguish EHRs from paper medical records and could be valuable to CMS's contractors when reviewing medical records. CMS concurred with our first recommendation and partially concurred with our second recommendation.

# TABLE OF CONTENTS

## OBJECTIVE

To describe how the Centers for Medicare & Medicaid Services (CMS) and its contractors implemented program integrity practices in light of electronic health records (EHRs) adoption.

## BACKGROUND

### Electronic Health Records

EHRs replace traditional paper medical records with computerized recordkeeping to document and store patient health information. EHRs may include patient demographics, progress notes, medications, medical history, and clinical test results from any health care encounter.[1]

EHRs may create new vulnerabilities, requiring CMS and its contractors to revise their approaches to protect against fraud and abuse. For example, clues within the progress notes, handwriting styles, and other attributes that help corroborate the authenticity of paper medical records are largely absent in EHRs. Further, tracing authorship and documentation in an EHR may not be as straightforward as tracing in a paper record. Health care providers can use EHR software features that may mask true authorship of the medical record and distort information in the record to inflate health care claims.

### CMS and Fraud Detection With EHRs

CMS uses administrative and program integrity contractors to pay claims, identify improper Medicare payments, and investigate fraud. These contractors include Medicare Administrative Contractors (MACs), Zone Program Integrity Contractors (ZPICs), and Recovery Audit Contractors (RACs).

*MACs.* MACs are responsible primarily for processing and paying Medicare claims.[2] MACs collaborate with CMS and other contractors to ensure that they pay claims correctly. MACs also educate providers on appropriate billing methods and are responsible for detecting and deterring fraud.

*ZPICs*. ZPICs are responsible primarily for detecting and deterring Medicare fraud.[3] ZPICs investigate providers that have filed potentially fraudulent claims by a variety of methods, including prepayment and

[1] CMS, *Electronic Health Records Overview*. Accessed at http://www.cms.gov on Jan. 11, 2011.

[2] CMS, *Part A and Part B Medicare Administrative Contractor Statement of Work, Attachment H-1, Master,* § C.4.4.a, September 2011.

[3] CMS, ZPIC IDIQ Umbrella Statement of Work, § 1.1.4, May 2009; CMS, *Medicare Program Integrity Manual*, Pub. No. 100-08, ch. 4, § 4.2.2.

postpayment reviews and onsite audits. They may also recommend that CMS or MACs revoke the billing privileges of providers.

*RACs.* RACs are responsible primarily for identifying and reducing Medicare improper payments by detecting and recouping improper payments made on claims of Medicare services.[4]

MACs, ZPICs, and RACs rely on medical records in aspects of their program integrity work. The transition from paper records to EHRs may require these contractors to adjust their techniques for identifying improper payments and investigating fraud.

### Ways EHRs May Facilitate Fraud

The full extent of health care fraud is unknown but it is substantial. The cost of health care fraud is between $75 billion and $250 billion. These figures are based on CMS estimates of total health care expenditures in 2009.[5] Experts in health information technology caution that EHR technology can make it easier to commit fraud.[6] Certain EHR documentation features, if poorly designed or used inappropriately, can result in poor data quality or fraud. Below we describe two examples of EHR documentation practices that could be used to commit fraud.

*Copy-Pasting*. Copy-pasting, also known as cloning, enables users to select information from one source and replicate it in another location.[7] When doctors, nurses, or other clinicians copy-paste information but fail to update it or ensure accuracy, inaccurate information may enter the patient's medical record and inappropriate charges may be billed to patients and third-party health care payers. Furthermore, inappropriate copy-pasting could facilitate attempts to inflate claims and duplicate or create fraudulent claims.

*Overdocumentation.* Overdocumentation is the practice of inserting false or irrelevant documentation to create the appearance of support for billing higher level services. Some EHR technologies auto-populate fields when using templates built into the system. Other systems generate extensive documentation on the basis of a single click of a checkbox, which if not appropriately edited by the provider may be inaccurate. Such features can

---

[4] CMS, *Medicare Program Integrity Manual*, Pub. No. 100-08, ch.1, § 1.3.1

[5] CMS, *National Health Expenditure Data*. Accessed at http://www.cms.gov on Jan. 3, 2012.

[6] Dougherty, Michelle. *HIT Policy Committee Hearing on Clinical Documentation*, February 13, 2013. Accessed at http://www.healthit.gov on March 19, 2013.

[7] Association of American Medical Colleges, Compliance Officers' Forum. *Appropriate Documentation in an EHR: Use of Information That Is Not Generated During the Encounter for Which the Claim Is Submitted: Copying/Importing/Scripts/Templates*. July 11, 2001.

produce information suggesting the practitioner performed more comprehensive services than were actually rendered.[8]

### Ways EHRs May Safeguard Against Fraud

Usage policies and technology features, if used consistently, could help prevent EHR fraud. However, providers that use EHR technology can often disable or bypass these features, making them ineffective. The Office of the National Coordinator for Health Information Technology (ONC), the office that coordinates the adoption, implementation, and exchange of EHRs, contracted with RTI International to develop recommended requirements for enhancing data quality in EHRs. Included in those recommendations are audit logs; access controls, including passwords; and export controls that restrict transferring information. The RTI recommendations highlight the importance of audit logs in fraud detection in that one-third of the individual criteria focus on the functions and features of audit logs.

Audit logs track changes within a record chronologically by capturing data elements, such as date, time, and user stamps, for each update to an EHR. An audit log can be used to analyze historical patterns that can identify data inconsistencies. To provide the most benefit in fraud protection, audit logs should always be operational, be stored as long as clinical records, and never be altered.

### Health Information Technology for Economic and Clinical Health Act

The Health Information Technology for Economic and Clinical Health Act was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), to support the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information.[9] Its goal is to achieve widespread adoption of EHRs by 2014.

To encourage EHR adoption, ARRA established the Medicare and Medicaid EHR incentive programs.[10] CMS will pay over $22.5 billion in incentive payments to eligible professionals and hospitals that demonstrate meaningful use of certified EHR technology. Medicare professionals and hospitals will face payment adjustments under Medicare starting in 2015

[8] Dougherty, Michelle. *HIT Policy Committee Hearing on Clinical Documentation*, February 13, 2013. Accessed at http://www.healthit.gov on March 19, 2013.
[9] P.L. 111-5, Title XIII.
[10] ARRA, Title IV, Pub L. 111-5.

for failing to successfully demonstrate meaningful use of certified EHR technology.[11]

### Related Office of Inspector General Work

The Office of Inspector General (OIG) released a companion report to this review that assessed the extent to which hospitals that have received EHR incentive payments implemented recommended fraud safeguards for EHR technology.[12]

In 2012, OIG released a report on physicians' reported use of EHR technology that found that 57 percent of Medicare physicians used an EHR at their primary practice locations in 2011. Additionally, three of every four Medicare physicians with an EHR system used a certified system to document evaluation and management services. [13] OIG is currently determining the extent to which documentation errors were facilitated by using EHR technology.[14]

In 2012, OIG released a study that found that CMS faces obstacles to overseeing the Medicare EHR incentive program that leave the program vulnerable to paying incentives to professionals and hospitals that do not fully meet the meaningful use requirements.[15]

In 2011, OIG released an audit of information technology (IT) controls in health IT standards. OIG found that ONC EHR certification criteria focused on IT security application controls for communication between EHR systems, but did not include basic, general IT security controls.[16]

## METHODOLOGY

### SCOPE

This study determined the extent to which the CMS administrative and program integrity contractors have adjusted program integrity efforts in light of EHR adoption.

---

[11] See §§ 1848(a)(7), 1853(l)(4), and 1886 (b)(3)(B), as enacted in ARRA. See also CMS, *CMS Finalizes Requirements for the Medicare EHR Incentive Program*. Accessed at http://www.cms.gov on Jan. 3, 2012.

[12] OIG, *Not All Recommended Safeguards Have Been Implemented in Hospital EHR Technology*, OEI-01-11-00570, December 2013.

[13] OIG, *Use of Electronic Health Record Systems in 2011 Among Medicare Physicians Providing Evaluation and Management Services*, OEI-04-10-00184, June 2012.

[14] OIG, OEI-04-10-00182, in progress.

[15] OIG, *Early Assessment Finds That CMS Faces Obstacles in Overseeing the Medicare EHR Incentive Program*, OEI-05-11-00250, November 2012.

[16] OIG, *Audit of Information Technology Security Included in Health Information Technology Standards*, A-18-09-30160, May 2011.

## Data Sources

*CMS Contractor Questionnaires*: We administered online questionnaires in January 2013 to three types of CMS administrative and program integrity contractors that use EHRs to pay claims, identify improper Medicare payments, and investigate fraud. We sent questionnaires to eight MACs, six ZPICs, and four RACs.[17] The questionnaires asked about their policies, procedures, and experiences with EHR fraud and Medicare claims. We asked about any procedures or review practices specific to EHRs. We had a 100-percent response rate.

*Document Review*: We reviewed guidance documents and policies on EHRs and fraud vulnerabilities that CMS and its contractors released for health care providers. We also reviewed CMS transmittals of new or changed policies and procedures relating to EHRs.

## Limitations

Our analysis used self-reported data from CMS contractors. We did not independently verify their statements.

## Standards

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

[17] Given that some of the contractors were transitioning both in and out of service, we consulted with CMS about which contractors we should contact for our study; therefore, the number of contractors that we contacted does not match the number currently operating.

## FINDINGS

# CMS and its contractors had adopted few program integrity practices specific to EHRs

Although EHR technology may make it easier to perpetrate fraud, CMS and its contractors have not adjusted their practices for identifying and investigating fraud in EHRs.

### *Few contractors were reviewing EHRs differently from paper medical records*

Although additional reviews are not required by CMS, two MACs and two ZPICs reported that they conduct them for EHRs beyond what they do for paper medical records. For example, the MACs reported that they confirm electronic signatures and request the providers' EHR protocols. The ZPICs reported that they request information about the providers' EHR technology and question the providers about their ability to access and alter the EHR data. (See Table 1.)

**Table 1: Number of CMS Contractors That Reported Conducting Additional Review Procedures**

| Contractor | Conduct Additional Review | Use Audit Log data |
|---|---|---|
| MAC | 2 out of 8 | 1 out of 8 |
| RAC | 0 out of 4 | 1 out of 4 |
| ZPIC | 2 out of 6 | 1 out of 6 |

Source: OIG analysis of contractors' responses to questionnaire, 2013.

Audit log data are unique to EHRs. They distinguish EHRs from paper records and could be valuable in authenticating the medical record that supports a claim. However, only 3 of the 18 Medicare contractors reported using audit log data as part of their reviews or investigative processes. For example, one contractor reported that it had used the audit log to verify that the provider had not changed the medical record after the date of care. Another contractor reviewed the audit log to validate authenticity of entries made in the medical record.

### *Not all contractors reported being able to determine whether a provider had copied language or overdocumented in a medical record*

MACs, ZPICs, and RACs reported varying ability to identify copied language and overdocumentation in both EHRs and paper medical records; however, ZPICs most often reported being able to identify such instances. (See Table 2.) Generally, more contractors reported being able to identify overdocumentation compared to copied language. Overdocumentation may be easier to identify because it is evident within the supporting medical record for a single claim. Contractors are unlikely to identify copied language in a single claim because it may require a single reviewer to examine multiple claims from a single patient or provider for evidence of copied language. ZPICs may be more successful at identifying potentially inappropriate practices because their primary objective is to target fraud and they are more likely to look at multiple claims as compared to other contractors. In addition, the other contractors refer instances of suspected fraud to ZPICs.

Opportunities for a provider to inappropriately copy-paste language and overdocument in a medical record for higher payment exist in paper medical records as well as EHRs. However, features in EHR technology make it easier for providers to copy-paste and overdocument in EHRs.

**Table 2: Number of CMS Contractors That Reported Being Able To Identify Copied Language and Overdocumentation**

| | Copied Language | | Overdocumentation | |
|---|---|---|---|---|
| **Type of Contractor** | **EHR** | **Paper Medical Record** | **EHR** | **Paper Medical Record** |
| MAC | 4 out of 8 | 4 out of 8 | 6 out of 8 | 5 out of 8 |
| ZPIC | 3 out of 6 | 6 out of 6 | 6 out of 6 | 6 out of 6 |
| RAC | 2 out of 4 | 1 out of 4 | 3 out of 4 | 3 out of 4 |

Source: OIG analysis of contractors' responses to questionnaire, 2013.

Among those contractors that could identify copied language and overdocumentation, not all reported taking followup actions after identifying these practices in both EHRs and paper medical records. Although all six ZPICs reported taking action after identifying copied language and overdocumentation, not all MACs and RACs did. Four MACs reported they referred the claims to the ZPICs; educated providers about proper documentation; and took administrative action, such as denial of payment. The two RACs that reported taking action sought further direction from CMS. About half of the ZPICs took administrative

action, such as overpayment adjustments, referrals to law enforcement, or referrals to CMS for payment suspension. The other ZPICs conducted additional interviews, additional physician reviews, or site visits.

## CMS had provided limited guidance to its contractors on fraud vulnerabilities in EHRs

Contractors reported receiving limited guidance from CMS in the past 2 years about fraud vulnerabilities, such as copied language, overdocumentation, and electronic signatures. (See Table 3.) Although MACs and RACs received guidance, ZPICs unanimously responded that CMS did not provide them with any. CMS did issue guidance to the contractors that states that "medical record keeping within an EHR deserves special considerations" and that "the original content, the modified content, and the date and authorship" must be identifiable. However, this guidance provides few details, and contractors described to OIG areas related to EHRs that require additional guidance.[18] Contractors noted proxy and electronic signatures (three MACs), EHR documentation (four MACs), and CMS's Electronic Submission of Medical Documentation Program (two ZPICs) as areas related to EHRs that they believe require additional CMS guidance.

**Table 3: Number of Contractors That Reported Receiving Guidance From CMS Related to EHRs**

| CMS Guidance | MAC | RAC | ZPIC |
|---|---|---|---|
| Copied language | 0 out of 8 | 2 out of 4 | 0 out of 6 |
| Overdocumentation | 1 out of 8 | 1 out of 4 | 0 out of 6 |
| Electronic signatures | 6 out of 8 | 3 out of 4 | 0 out of 6 |
| Other EHR-related guidance | 2 out of 8 | 1 out of 4 | 0 out of 6 |

Source: OIG analysis of contractors' responses to questionnaire, 2013.

[18] CMS Manual System, Pub. No. 100-08, *Medicare Program Integrity*, Transmittal 442. December 7, 2012.

## CONCLUSION AND RECOMMENDATIONS

The Department of Health and Human Services has spent considerable resources to promote widespread adoption of EHRs, including developing certification criteria and defining meaningful use for EHR technology while paying over $22.5 billion in incentive payments. It has directed less attention to addressing potential fraud and abuse vulnerabilities in EHRs despite the challenges they pose to the integrity of medical records.

Our findings show that CMS and its contractors have not changed their program integrity strategies in light of EHR adoption. Some CMS contractors reported that they were unable to identify copied language and overdocumentation in a medical record. This is a particular concern with EHRs because such documentation practices are made easier in an electronic environment. In addition, few CMS contractors have adopted additional review procedures for EHRs. Finally, CMS has offered limited guidance to CMS contractors on fraud vulnerabilities.

We recommend that CMS:

### Provide guidance to its contractors on detecting fraud associated with EHRs

Although CMS has communicated to contractors through manuals that "medical record keeping within an EHR deserves special considerations" and that "the original content, the modified content, and the date and authorship" must be identifiable, it has provided contractors with limited guidance regarding the review of EHR-based claims. CMS could work with contractors to identify best practices and develop guidance and tools for detecting fraud associated with EHRs. Specific guidance should address EHR documentation and electronic signatures in EHRs.

### Direct its contractors to use providers' audit logs

Audit log data are unique to EHRs and distinguish EHRs from paper medical records. Audit logs could be a source of information for CMS's contractors when reviewing medical records. Audit log data could be valuable in authenticating the medical record that supports a claim.

## AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

CMS concurred with our first recommendation and partially concurred with our second recommendation.

To address our recommendation that CMS provide guidance to its contractors on detecting fraud associated with EHRs, CMS stated that intends to develop guidance on the appropriate use of the copy-paste feature in EHRs. It also stated that it will work with its contractors to identify best practices for detecting fraud associated with EHRs. Our recommendation referenced guidance specific to EHR documentation and electronic signatures in EHRs. We ask CMS to address guidance on these issues in its final management decision.

In response to our second recommendation, that CMS direct its contractors to use audit logs, CMS acknowledged that audit logs can be one of several tools to ensure the accuracy and validity of information in EHRs. It also stated that the use of audit logs may not be appropriate in every circumstance and that review of audit logs requires special training. CMS stated that it is working with its contractors, EHR experts, and ONC-sponsored workgroups to consider issues presented by digital clinical data, including determining the authenticity of information in EHRs. We agree that audit logs should be part of a comprehensive approach to reviewing authenticity of EHRs and understand the challenges that CMS and its contractors face to use audit logs. We reiterate our recommendation that CMS make audit logs part of its contractors' reviews of EHRs.

For a full text of CMS's comments, see Appendix A.

# APPENDIX A

## Agency Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

*Administrator*
Washington, DC 20201

**DATE:** NOV 22 2013

**TO:** Daniel R. Levinson
Inspector General

**FROM:** Marilyn Tavenner /S/
Administrator

**SUBJECT:** Office of Inspector General (OIG) Draft Report: "CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs" (OEI-01-11-00571)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the above-referenced OIG draft report. The purpose of this report is to describe how CMS and its contractors implemented program integrity practices in light of electronic health records (EHRs) adoption.

The CMS is committed to preventing fraud, waste, and abuse in EHRs. CMS has issued guidance to its contractors that states that "medical record keeping within an EHR deserves special considerations" and that "the original content, the modified content, and the date and authorship" must be identifiable (http://www.cms.gov/regulations-and guidance/guidance/transmittals/downloads/r442pi.pdf.). However, CMS realizes that additional guidance is needed and intends to work with its contractors in the development of effective guidance and tools in an effort to detect fraud vulnerabilities in the area of EHRs.

Our response to each of the OIG recommendations follows.

**OIG Recommendation:**

CMS should provide guidance to its contractors on detecting fraud associated with EHRs.

**CMS Response:**

The CMS concurs with this recommendation. CMS has been actively considering the issue of preventing fraud, waste, and abuse in EHRs. In May 2013, CMS and ONC held a public listening session with stakeholders about a number of issues pertaining to billing and coding for EHRs, including the impact of EHRs on clinical documentation. Given its potential for use in fraud, CMS intends to develop appropriate guidelines to ensure appropriate use of the copy paste feature in EHRs. CMS will also consider whether additional guidance and tools are needed to

help detect fraud associated with EHRs. CMS will continue its program integrity efforts at addressing fraud, waste, and abuse by continuing to work with its contractors to identify best practices for detecting fraud associated with EHRs.

**OIG Recommendation:**

CMS should direct its contractors to use providers' audit logs.

**CMS Response:**

The CMS partially concurs with the recommendation. Audit logs can be one of several important tools in ensuring that information included in EHRs are valid and authentic. However, use of audit logs may not be appropriate in every circumstance and should be part of a comprehensive approach to reviewing the authenticity of EHRs. Review of audit logs requires reviewers to obtain training to interpret and reconstruct the history of each medical record supplied in an electronic format and supported by a log.

The CMS has been engaged with the staff, its contractors, and EHR experts as well as the Standards and Interoperability workgroups sponsored by the Office of the National Coordinator to consider the unique issues presented by digital clinical data, including determining authenticity of information in EHRs.

Again, we appreciate the opportunity to comment on this draft report and look forward to working with OIG on this and other issues.

## ACKNOWLEDGMENTS

This report was prepared under the direction of Joyce Greenleaf, Regional Inspector General for Evaluation and Inspections in the Boston regional office; Kenneth Price, Deputy Regional Inspector General; and Russell Hereford, Deputy Regional Inspector General.

Danielle Fletcher served as the team leader for this study. Other Office of Evaluation and Inspections staff from the Boston regional office who conducted the study include Kimberly Yates. Central office staff who provided support include Kevin Manley and Clarence Arnold.

# Office of Inspector General

http://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 assessments 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.