Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

OCR SHOULD STRENGTHEN ITS FOLLOWUP OF BREACHES OF PATIENT HEALTH INFORMATION REPORTED BY COVERED ENTITIES

Suzanne Murrin
Deputy Inspector General for Evaluation and Inspections

September 2015
OEI-09-10-00511

EXECUTIVE SUMMARY: OCR SHOULD STRENGTHEN ITS FOLLOWUP OF BREACHES OF PATIENT HEALTH INFORMATION REPORTED BY COVERED ENTITIES
OEI-09-10-00511

WHY WE DID THIS STUDY

Recent news illustrates that a data breach can affect millions of individuals. Breaches of protected health information (PHI)—such as patients' names, test results, medical conditions, prescriptions, or treatment histories—could expose patients to privacy invasion, fraud, identity theft, and/or other harm. The Breach Notification Rule of the Health Insurance Portability and Accountability Act (HIPAA), along with HIPAA's Privacy and Security Rules, established HIPAA standards that aim to safeguard PHI. The Breach Notification Rule requires that covered entities report breaches of unsecured PHI to the Office for Civil Rights (OCR). OCR's oversight of covered entities' compliance with the HIPAA standards is critical to help ensure that covered entities address the problems that led to breaches.

HOW WE DID THIS STUDY

To assess OCR's oversight of covered entities that reported breaches, we (1) reviewed a statistical sample of large breaches (i.e., breaches affecting 500 or more individuals) and small breaches (i.e., breaches affecting fewer than 500 individuals) that covered entities reported to OCR from September 2009 through March 2011; (2) surveyed OCR staff; and (3) interviewed OCR officials. We also reviewed OCR's investigation policies. We surveyed a statistical sample of Medicare Part B providers and reviewed documents that they provided to determine the extent to which they addressed three selected breach administrative standards.

WHAT WE FOUND

OCR should strengthen its followup of breaches of PHI reported by covered entities. OCR investigated the large breaches, as required, and in almost all of the closed large-breach cases, it determined that covered entities were noncompliant with at least one HIPAA standard. Although OCR documented corrective action for most of the closed large-breach cases in which it made determinations of noncompliance, 23 percent of cases had incomplete documentation of corrective actions taken by covered entities. OCR also did not record small-breach information in its case-tracking system, which limits its ability to track and identify covered entities with multiple small breaches. Although 61 percent of OCR staff checked at least sometimes as to whether covered entities had reported prior large breaches, 39 percent rarely or never did so. If OCR staff wanted to check, they may face challenges because its case-tracking system has limited search functionality and OCR does not have a standard way to enter covered entities' names in the system. Finally, from our review of the documents that Medicare Part B providers submitted, most addressed all three selected breach administrative standards but 27 percent did not. These providers may not be adequately safeguarding PHI.

WHAT WE RECOMMEND

OCR should (1) enter small-breach information into its case-tracking system or a searchable database linked to it; (2) maintain complete documentation of corrective action; (3) develop an efficient method in its case-tracking system to search for and track covered entities that reported prior breaches; (4) develop a policy requiring OCR staff to check whether covered entities reported prior breaches; and (5) continue to expand outreach and education efforts to covered entities. OCR concurred with all five recommendations and described its activities to address them.

TABLE OF CONTENTS

OBJECTIVES

1. To assess the Office for Civil Rights' (OCR) oversight of covered entities that reported breaches of protected health information (PHI).
2. To determine the extent to which Medicare Part B providers addressed three selected breach administrative standards.

BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA) includes the Breach Notification Rule, Privacy Rule, and Security Rule.[1] These rules established breach, privacy, and security standards, which aim to safeguard health information. We collectively refer to these standards as HIPAA standards. In general, the Breach Notification Rule requires that covered entities—such as doctors, pharmacies, and health insurance companies—make certain notifications when they discover a breach of unsecured protected health information (PHI)[2] and follow standards that safeguard PHI. A breach of unsecured PHI is the unauthorized access or use of individually identifiable health information that has not been destroyed or rendered indecipherable.[3]

OCR is responsible for overseeing covered entities' compliance with the HIPAA standards, including the Breach Notification Rule. OCR oversight is critical given the increased use of health information technologies, such as electronic health records, and the potential for breaches that may result in an invasion of privacy, identity theft, or other fraud. In a report to Congress, covered entities reported to OCR more than 78,000 breaches

[1] The Breach Notification Rule was established by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which was enacted as part of the American Recovery and Reinvestment Act of 2009, P.L. No. 111-5. 45 CFR pt. 164, subpt. D. The Privacy Rule establishes national standards to protect individuals' medical records and other personal health information. An example of a privacy standard is safeguarding health information by using locks and keys to secure medical records. 45 CFR pt. 164, subpt. E. The Security Rule establishes national standards to protect individuals' electronic personal health information. An example of a security standard is properly disposing of electronic media or devices that maintain health information. 45 CFR pt. 164, subpt. C.

[2] Unsecured PHI is individually identifiable health information (in electronic, oral, or paper form) that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of encryption or destruction such as shredding. Examples of PHI include an individual's name, Medicare number, or medical history. 45 CFR § 160.103.

[3] HITECH Act, § 13400(l).

from when the Breach Notification Rule went into effect in September 2009 to the end of 2012.[4]

Covered Entities

The Breach Notification Rule applies to three types of covered entities.[5] Covered entities are defined as (1) health plans, (2) health care clearinghouses, and (3) health care providers that transmit health information in electronic form in connection with a HIPAA-covered transaction.[6] Health plans are individual or group plans that provide or pay for medical care, and include governmental plans, such as Medicare and Medicaid.[7] Health care clearinghouses include businesses that process or help to process health information received from another covered entity, as well as businesses that receive HIPAA-covered transactions from another covered entity.[8] Examples of health care clearinghouses are companies that provide services related to billing, claims processing, or the management of health information. Health care providers include individual practitioners (including those who participate in the Medicare and Medicaid programs), hospitals, and pharmacies.[9]

Breach Notification Rule Standards for Covered Entities

Covered entities must comply with standards established in the Breach Notification Rule (breach standards). The breach standards include notification standards and administrative standards, and apply to breaches occurring on or after September 23, 2009.

The notification standards require that, in the event of a breach, covered entities notify individuals affected by the breach, the Secretary of Health and Human Services, and the media.[10, 11] Covered entities must provide written notification to individuals affected by the breach without unreasonable delay and in no case later than 60 days after discovery of the

---

[4] 74 Fed. Reg. 42740–42770 (Aug. 24, 2009). OCR, *Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2011 and 2012*. Accessed at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf on June 19, 2015.

[5] The Breach Notification Rule also applies to covered entities' business associates. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. 45 CFR § 160.103.

[6] HIPAA-covered transactions generally consist of billing and payments for services or insurance coverage. Examples of HIPAA-covered transactions include patient enrollment, claims, benefits, and eligibility inquiries. 42 U.S.C. 1320d-2(a)(2).

[7] 45 CFR § 160.103.

[8] Ibid.

[9] Ibid. Social Security Act, § 1172(a)(3), 42 U.S.C. 1320d-1(a)(3).

[10] 45 CFR pt. 164, subpt. D.

[11] The notification standards also require business associates (see footnote 5) to notify covered entities of a breach.

breach.[12] They must also notify the Secretary of Health and Human Services—via OCR—of any breaches affecting 500 or more individuals (large breaches) without unreasonable delay,[13] and annually notify OCR of any breaches affecting fewer than 500 individuals (small breaches).[14] In the event of a large breach, covered entities must also notify prominent media outlets.[15]

The breach administrative standards outline covered entities' responsibilities for safeguarding PHI. These standards address when and how covered entities can use, share, and disclose PHI, and how covered entities should secure PHI.[16]

OCR Oversight of Covered Entities

OCR's oversight of covered entities depends primarily on covered entities' self-reporting of breaches. OCR's oversight role also includes responding to complaints, tips, or media reports about breaches. Pursuant to OCR policy, OCR must investigate large breaches but is not required to investigate small breaches. Also, the HITECH Act requires OCR to offer guidance and education to covered entities on their rights and responsibilities related to privacy and security standards that aim to prevent breaches of PHI.[17]

OCR Investigation of Breach Cases. OCR may open a breach case after a covered entity reports a breach to OCR. The breach report includes information such as the covered entity's name; the type of covered entity; the estimated number of individuals affected by the breach; the type of breach (e.g., theft, hacking, or unauthorized access); and any corrective action taken by the covered entity in response to the breach. OCR verifies this information and then initiates its breach investigation.

OCR has discretion on how to investigate breach cases and the techniques it uses include, but are not limited to, conducting interviews, document reviews, and onsite visits.[18] During its investigation, OCR determines the cause of the breach and whether the covered entity complied with the HIPAA standards. It may check whether a covered entity reported prior

[12] 45 CFR §§ 164.400 and 164.404.

[13] 45 CFR § 164.408. For large breaches, covered entities must notify the Secretary of Health and Human Services without unreasonable delay and in no case later than 60 days following the breach.

[14] OCR requires covered entities to maintain a log or other documentation of any small breaches and to submit the information to OCR no later than 60 days after the end of the calendar year during which the breaches were discovered. 45 CFR § 164.408.

[15] 45 CFR § 164.406.

[16] 45 CFR § 164.414.

[17] HITECH Act, § 13403.

[18] 45 CFR § 160.310(c)(1).

breaches. When appropriate, OCR may provide technical assistance to covered entities. This technical assistance may include, but is not limited to, helping the covered entity understand the HIPAA standards.[19]

OCR Resolutions of Breach Cases. After OCR investigates, it may resolve a breach case with a determination of no violation of HIPAA standards, or, if there is an indication of noncompliance with standards, by requesting that the covered entity take corrective action.[20] A determination of no violation means that OCR did not identify a violation of the standards or that the evidence was insufficient to make a determination of a violation. A determination that the covered entity should take corrective action indicates that the covered entity may not have complied with at least one HIPAA standard. Corrective action can include retraining staff on existing PHI policies, revising policies, and training staff on these new policies. Because OCR may investigate more than one standard per breach case, a single investigation can result in multiple determinations.

OCR may also resolve a breach case by entering into a resolution agreement with the covered entity.[21] Resolution agreements typically require that the covered entity take corrective action. In more serious circumstances, OCR may impose a civil monetary penalty (CMP) on a covered entity.[22, 23] In determining a CMP amount, OCR may consider, among other factors, whether the current breach was similar to other breaches reported by the covered entity, or if the covered entity has a history of noncompliance with the HIPAA standards.[24]

If OCR makes a determination that the covered entity did not violate the HIPAA standards, OCR may close the case. If OCR makes a determination of noncompliance, it may request that the covered entity take appropriate corrective action. OCR would then close the case after it concludes that the covered entity has taken such action.

---

[19] 45 CFR § 160.304(b).

[20] 45 CFR § 160.312.

[21] A resolution agreement is a contract—signed by OCR and a covered entity—in which the covered entity agrees to perform certain obligations (e.g., staff training) and to submit progress reports to OCR, generally for a period of 3 years. OCR, *Resolution Agreements*. Accessed at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html on June 5, 2015.

[22] For example, OCR may impose a CMP if a covered entity fails to implement all of the corrective actions or was uncooperative with the investigation.

[23] 45 CFR pt. 160, subpt. D.

[24] 45 CFR § 160.408.

OCR Program Information Management System

OCR staff use the Program Information Management System (PIMS) to electronically document their investigation of breach cases.[25] Specifically, they use this case-tracking system to record (1) action that OCR staff and the covered entity take, (2) evidence gathered during the investigation, (3) OCR's determinations, and (4) any supporting documents that OCR receives from the covered entity. OCR's policy is to ensure that staff include in PIMS the documentation of covered entities' corrective action. OCR staff can also use PIMS to search for prior breaches or other HIPAA-related investigations of covered entities.

Related OIG Work

This report is part of the Office of Inspector General's (OIG's) body of work on the security of health information. In a May 2011 report, OIG found that electronic PHI in seven hospitals was vulnerable to unauthorized access, use, and disclosure.[26] In a November 2013 report, OIG found that OCR did not meet all Federal requirements in its oversight and enforcement of the Security Rule.[27] Additionally, in conjunction with this report, OIG is issuing a report on OCR's oversight of covered entities' compliance with standards established by the Privacy Rule.[28]

METHODOLOGY

Data Collection and Analysis

To assess OCR's oversight of covered entities that reported breaches of PHI, we (1) reviewed a statistical sample of large and small breaches, respectively, that covered entities reported to OCR; (2) surveyed OCR staff; and (3) interviewed OCR officials. To supplement our understanding of OCR's investigation process, we reviewed OCR's policies and procedures. To determine the extent to which covered entities addressed three selected breach administrative standards, we surveyed and collected documents from a statistical sample of Part B providers. See

[25] 67 Fed. Reg. 57011–57012 (Sept. 6, 2002).

[26] At the time of the audit, the Centers for Medicare & Medicaid Services (CMS) had oversight authority for the HIPAA Security Rule. The report was issued to OCR because the HITECH Act redelegated oversight and enforcement of the HIPAA Security Rule from CMS to OCR. OIG, *Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight*, A-04-08-05069, May 2011. Accessed at http://oig.hhs.gov/oas/reports/region4/40805069.pdf on June 19, 2015.

[27] OIG, *The Office for Civil Rights Did Not Meet All Federal Requirements in Its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule*, A-04-11-05025. Accessed at http://oig.hhs.gov/oas/reports/region4/41105025.pdf on June 19, 2015.

[28] OIG, *OCR Should Strengthen Its Oversight of Covered Entities' Compliance With the HIPAA Privacy Standards*, OEI-09-10-00510.

Appendix A for the detailed methodology and Appendix B for the point estimates and confidence intervals. We project our estimates at the 95-percent confidence level.

Review of Large Breaches. We reviewed large breaches that covered entities reported to OCR to determine how OCR investigated and resolved them, and to determine the extent to which OCR documented covered entities' corrective action in PIMS. We selected a simple random sample of 100 large breaches from a population of 264 large breaches that covered entities reported to OCR during the period of September 23, 2009, to March 31, 2011. We focused our analysis on the large-breach cases that had been closed. Except where noted, we project our estimates to the subpopulations of (1) closed large-breach cases and (2) closed large-breach cases in which OCR made determinations of noncompliance.

Review of Small Breaches. We reviewed small breaches that covered entities reported to OCR to determine how OCR investigated and resolved them. We selected a simple random sample of 150 small breaches from a population of 30,284 small breaches that covered entities reported to OCR during the period of September 23, 2009, to March 31, 2011. We project our estimates of the small breaches to this population.

Survey of OCR staff. We surveyed all 83 OCR staff who worked on breach cases and asked how they investigated these cases. We had a 100-percent response rate. Of the 83 OCR staff, 61 reported that they worked on large breaches and 52 reported that they worked on small breaches.[29]

Interviews With OCR Officials and Review of OCR Documents. We interviewed OCR officials to understand how OCR investigates breach cases, and we reviewed OCR's policies and procedures to supplement our understanding of OCR's investigation process.

Survey of Part B Providers. We reviewed survey responses and documents submitted to OIG from a statistical sample of Part B providers to determine the extent to which they addressed three selected breach administrative standards that require them to have:

(1) established a sanctions policy for staff;

(2) provided all staff with training on the covered entity's policies and procedures with respect to PHI; and

[29] These two figures are not mutually exclusive, as OCR staff worked on one or both types of breach cases.

(3) implemented policies and procedures.[30]

We selected a simple random sample of 150 Part B providers from the population of 913,235 Part B providers that submitted at least 1 Medicare claim in 2011. We administered an electronic survey to our sample of Part B providers and obtained 132 responses, an 88-percent response rate. We project our estimates to 88 percent of our population, which is about 803,647 Part B providers that submitted at least 1 Medicare claim in 2011.

Limitations

Our analysis of the breach cases is limited to the information provided by OCR. We did not contact covered entities to verify information regarding breach cases, such as corrective action that was recorded in PIMS. We did not determine whether each breach case was appropriately resolved by OCR staff. We did not examine the determinations reached by OCR or the corrective action taken in prior breach cases that involved the same covered entities. Our analysis of the OCR staff survey is from self-reported data. Our analysis of the Part B provider survey is from self-reported data and documents submitted by Part B providers.

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.

[30] These three breach administrative standards are located at 45 CFR §§ 164.530(e)(1), 164.530(b)(1), and 164.530(i)(1).

FINDINGS

OCR investigated all large breaches, as required; however, OCR did not record small-breach information in its case-tracking system, which limits its ability to track and identify covered entities with multiple small breaches

OCR followed its policy of investigating large breaches that were reported by covered entities. OCR opened a case for each of the large breaches in our sample and investigated them.[31] It closed 69 percent of these large-breach cases; the remaining 31 percent of large-breach cases were open at the time of our review. The closed large-breach cases in our sample involved 68 covered entities and affected more than 1.1 million individuals.

OCR investigated the large-breach cases by reviewing documents and/or contacting individuals involved in the cases. For the closed large-breach cases that were in our sample, OCR staff frequently requested and reviewed documents from covered entities, such as policies and procedures related to the appropriate use and disclosure of PHI. Also, OCR staff often conducted phone interviews to gather information needed for the investigation. Although OCR has authority to conduct onsite visits, it did not do so for any of the closed large-breach cases that were in our sample.

OCR did not record information about small breaches in PIMS, nor did it investigate the small breaches that covered entities reported to OCR.[32] Without including information about the small breaches in PIMS, OCR cannot effectively identify covered entities that have a history of noncompliance with the HIPAA standards. Although OCR has authority to investigate small breaches, it did not do so in any of the cases that were in our sample.

[31] We project with 95-percent confidence that OCR investigated between 97 percent and 100 percent of all large-breach cases in our population of large breaches.

[32] We project with 95-percent confidence that OCR investigated between 0 percent and 2 percent of all small breaches in our population of small breaches.

In almost all of the closed large-breach cases, OCR determined that covered entities were noncompliant with at least one HIPAA standard

OCR determined that covered entities were noncompliant with at least one HIPAA standard in 93 percent of closed large-breach cases.[33] Among these cases that were in our sample, the most common type of noncompliance was the failure to implement the safeguard-related privacy and/or security standards. Such noncompliance may result in an invasion of privacy, identity theft, or other harm.

OCR staff worked with covered entities to identify corrective action needed to address the noncompliance. Examples of these corrective action included training or retraining staff on safeguarding PHI, performing risk assessments, and implementing policies on notifying affected individuals. OCR staff also provided some covered entities with technical assistance. Although OCR has authority to enter into resolution agreements with covered entities and to impose CMPs, it did not use either of these mechanisms for the closed large-breach cases in our sample in which it had made determinations of noncompliance.[34]

OCR documented corrective action for about three-quarters of closed large-breach cases in which it made determinations of noncompliance; however, 23 percent of cases had incomplete documentation

OCR lacked complete documentation in PIMS of corrective action for 23 percent of closed large-breach cases in which it determined that covered entities were noncompliant. For the remaining 77 percent, OCR had complete documentation in PIMS of corrective action. Without complete documentation, OCR cannot verify whether covered entities took corrective action to address noncompliance with the HIPAA standards.

[33] The remaining 7 percent of closed large-breach cases include 6 percent in which OCR determined that covered entity did not violate the HIPAA standards (i.e., OCR did not identify a violation or the evidence was insufficient to make a determination of a violation), and 1 percent that involved an entity not covered by HIPAA.

[34] After we conducted our data collection, OCR entered into resolution agreements with seven covered entities as the result of investigations opened in response to breach reports that occurred from 2009 through 2012. OCR, *Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2011 and 2012*. Accessed at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf on June 22, 2015.

Sixty-one percent of OCR staff checked at least sometimes as to whether covered entities had reported prior large breaches; however, 39 percent rarely or never did so

Although OCR staff have the discretion to check whether a covered entity has reported prior large or small breaches, many reported that they rarely or never did so. Thirty-nine percent of OCR staff reported that they rarely or never checked whether a covered entity had reported prior large breaches. The reasons they gave for rarely or never checking varied, including that they thought that other OCR staff might have already checked for prior breaches, that they did not think prior breaches were relevant to the investigation, and/or that there was no efficient way to search for covered entities in PIMS. Checking whether a covered entity has reported prior breaches—large and/or small—may help OCR staff identify those that have a history of noncompliance with the HIPAA standards. See Table 1 for the percentages of OCR staff who checked at various frequencies as to whether a covered entity reported prior large and small breaches.

Table 1: Percentages of OCR staff who checked at various frequencies as to whether a covered entity had reported prior large or small breaches

Frequency of checking for prior breaches reported by a covered entity	Percentage of OCR staff who checked for prior large breaches	Percentage of OCR staff who checked for prior small breaches
Rarely or never	39%	50%
Usually or sometimes	38%	29%
Always	23%	21%
Total	**100%**	**100%**

Source: OIG analysis of data from survey of OCR staff, 2015.

From September 2009 through March 2011, some covered entities reported multiple breaches to OCR. From our population of large-breach cases, we identified 15 covered entities that reported multiple large breaches to OCR. One of these covered entities reported three large breaches that affected more than 500,000 individuals.[35] From our sample of small breaches, we identified six covered entities that reported multiple small breaches to OCR. They reported between 2 and 18 small breaches to OCR. Because covered entities are required to report small breaches only annually, OCR may not know for up to a year that a covered entity has had multiple small breaches. Without checking whether a covered

[35] The numbers of affected individuals is approximate because some covered entities reported being uncertain about the number of individuals affected by a breach. Accessed at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf on July 21, 2015.

entity has reported multiple large and/or small breaches, OCR cannot identify entities that may have systemic issues in safeguarding PHI.

OCR's case-tracking system has limited search functionality

OCR staff reported that PIMS has limited functionality when searching for covered entities. Variations in how OCR staff enter a covered entity's name into PIMS (e.g., abbreviations and capitalization) may limit OCR staffs' ability to identify covered entities that reported multiple breaches. For example, one OCR staff person may enter ABC Company into PIMS as "ABC Company, Inc." while another may enter it as "ABC Co., Inc." or "ABC Comp." As a result, a single covered entity could appear in PIMS as three different covered entities. An OCR official explained that OCR staff may need to enter all possible variations of a covered entity's name to identify any prior breaches reported by a covered entity. Without a standard method to search for and track covered entities in PIMS, OCR may not be able to identify covered entities that have a history of noncompliance, which is one of the factors that OCR can use to determine the amount of a CMP.

Almost three-quarters of Part B providers addressed all three selected breach administrative standards; however, 27 percent of Part B providers did not

According to our analysis of supporting documents that Part B providers submitted, 27 percent of Part B providers did not address all three selected breach administrative standards. By not addressing these standards, Part B providers could be placing PHI at risk of misuse or inappropriate disclosure. Because OCR relies on covered entities' self-reporting of breaches, OCR may not be aware of Part B providers—or covered entities, in general—that do not address the breach administrative standards. See Table 2 for the percentages of Part B providers that did not address the selected breach administrative standards.

Table 2: Percentage of Part B providers that did not address each of the selected breach administrative standards

Selected breach administrative standard	Percentage of Part B providers that did not address the standard
Established sanctions policy for staff	24%
Provided some or all staff with training on the covered entities' policies and procedures with respect to PHI	21%
Implemented PHI policies and procedures that complied with the Breach Notification Rule	17%

Source: OIG analysis of data from survey of Part B providers, 2015.

The remaining 74 percent of Part B providers addressed all three selected breach administrative standards. As examples of how they addressed the selected breach administrative standards, Part B providers submitted to OIG their organizational policies on protecting patient health information and handling breaches, their training materials on the HIPAA standards, and their policies on sanctions for employees who fail to safeguard PHI.

Sixty-two percent of Part B providers expressed interest in learning more about OCR and the Breach Notification Rule. Some Part B providers were interested in receiving additional information on the breach standards such as sample policies and procedures, examples of notifications, and other providers' best practices. Thirty-five percent of Part B providers reported that they were unfamiliar with OCR's jurisdiction over the Breach Notification Rule. Without knowing that OCR has this jurisdiction, Part B providers may not be aware of—and may not access—OCR resources on how to comply with the Breach Notification Rule.

CONCLUSION AND RECOMMENDATIONS

As we have seen in recent media reports, a single data breach can affect millions of individuals. Breaches of PHI could expose patients to privacy invasion, fraud, identity theft, or other harm. OCR oversight of covered entities' compliance is critical to help ensure that covered entities provide the required notifications, address the problems that led to breaches, and comply with the HIPAA standards.

OCR should strengthen its followup of breaches of PHI reported by covered entities. OCR followed its policy of investigating the large breaches that covered entities reported to it. In almost all of the closed large-breach cases that OCR investigated, it determined that covered entities were noncompliant with at least one HIPAA standard. Although OCR documented corrective action for most of the closed large-breach cases in which it made determinations of noncompliance, 23 percent of cases had incomplete documentation of corrective actions taken by covered entities. OCR also did not record small-breach information in PIMS, which limits its ability to track and identify covered entities with multiple small breaches. Further, although 61 percent of OCR staff checked at least sometimes as to whether covered entities had reported prior large breaches, 39 percent rarely or never did so. If OCR staff wanted to check for prior breaches, they may face challenges because OCR does not have a standard way to enter covered entities' names in PIMS. Lastly, because OCR relies on covered entities to self-report breaches, it may not be aware of the Part B providers that we identified as not addressing three selected breach administrative standards.

We recommend that OCR:

Enter information regarding the small breaches into PIMS or a searchable database linked to PIMS

This could enable OCR staff to electronically track small breaches in PIMS or a searchable database linked to PIMS. OCR could use this information to identify and oversee covered entities that report multiple small breaches. Covered entities that report multiple small breaches may be experiencing systemic problems that compromise PHI.

Maintain complete documentation in PIMS of corrective actions

OCR should maintain complete documentation in PIMS of corrective actions. OCR should develop a process—e.g., a checklist—in PIMS to identify the corrective-action documentation that it receives and the documentation that covered entities still need to submit. Having complete documentation could enable OCR to verify whether a covered entity took corrective action to address noncompliance.

Develop an efficient method in PIMS to search for and track covered entities that reported prior breaches

To effectively record, track, and search for covered entities that reported prior breaches, OCR could enter unique provider identifiers in PIMS, such as the National Provider Identifier or Employer Identification Number.[36] This could resolve problems with variations in how OCR staff enter and search for a covered entity's name in PIMS. It would also assist in identifying covered entities with a history of noncompliance.

Develop a policy requiring OCR staff to check whether covered entities reported prior breaches

If OCR staff check whether a covered entity has reported other breaches, they could identify those that may have systemic problems in safeguarding PHI. Covered entities that reported multiple large and/or small breaches to OCR may not be addressing underlying privacy or security issues. Once it identifies covered entities with multiple breaches, then OCR could initiate compliance reviews and/or conduct onsite visits, as appropriate. In addition, OCR could consider a covered entity's history of noncompliance in determining an appropriate resolution, such as entering into a resolution agreement or imposing a CMP.

Continue to expand outreach and education efforts to covered entities such as Part B providers

To improve covered entities' compliance with the HIPAA standards, OCR could target industry and professional health care associations to educate covered entities about OCR and the HIPAA standards. OCR could (1) conduct additional presentations for these associations; (2) continue to use electronic media—such as posting information on its Web site or sending updates via its listserv—to announce recent changes to the HIPAA standards; (3) continue to provide resources, such as Web seminars on compliance and how to prevent breaches, and templates of various breach policies and procedures; and (4) assess the impact of its outreach and education efforts to focus on those that OCR determines to be effective. OCR could also work with CMS—the agency that oversees Medicare—to increase Part B providers' compliance with the HIPAA standards.

[36] HIPAA required employers to have standard national numbers that identify them on general transactions. CMS selected the Employee Notification Number as the identifier for employers, effective July 2002.

AGENCY COMMENTS

OCR concurred with all five of OIG's recommendations and described ongoing activities in support of them. As of September 2015, OCR reported that its case-tracking system has been upgraded, which enables OCR staff to capture small-breach information in a database and to search for and track covered entities' history of compliance. OCR also reported that it is working on implementing policies to ensure that when staff investigate cases, they review the covered entity's history of investigations. In addition, OCR indicated that it will work to ensure that all OCR staff who investigate cases understand the appropriate procedures for maintaining documentation of corrective action in PIMS.

See Appendix C for the full text of OCR's comments.

APPENDIX A

Detailed Methodology

Scope

We reviewed a sample of large and small breaches reported to OCR by covered entities during the period of September 23, 2009, to March 31, 2011. Our review focused on the large breach cases that OCR had closed by the time of our review, and cases in which OCR made determinations of noncompliance.

We surveyed and requested documents from a sample of Part B providers that submitted at least one Medicare claim in 2011.[37] We selected three breach administrative standards covered by the Breach Notification Rule for which we could collect from providers documentation showing that they addressed the standards.

Data Collection and Analysis

We used five data sources for our evaluation: (1) a review of large breaches that covered entities reported to OCR, (2) a review of small breaches that covered entities reported to OCR, (3) a survey of OCR staff, (4) interviews with OCR officials and a review of OCR's policies and procedures for investigating breach cases, and (5) a survey of Part B providers.

Review of Large Breaches. We requested from OCR a list of all large breaches that covered entities reported to OCR during the period of September 23, 2009, to March 31, 2011. We received from OCR a list of 264 large breaches. We selected a simple random sample of 100 large breaches from this population, and we requested that OCR provide us with all data (e.g., action that OCR and the covered entity took, evidence gathered during the investigation, OCR determinations, and any supporting documentation from the covered entity) for each of the large breaches. OCR did not provide OIG with any other documentation (e.g., paper files) outside of the PIMS case data.

We reviewed the large breaches that covered entities reported to OCR to determine whether OCR investigated them and estimated the percentage of large breaches that OCR investigated. We considered a large breach to be a large-breach case if OCR investigated it. We categorized each of the 100 large-breach cases as open or closed. We considered a large-breach case to be open if it was open as of April 17, 2012, the date on which we

[37] Part B providers may include doctors, nurse practitioners, and physical therapists. We focused on Part B providers because (1) OCR does not have a list of all covered entities under its jurisdiction, (2) Part B providers were the population for which a list was available, and (3) Part B providers are covered entities.

received the large-breach case data from OCR. We considered a large-breach case to be closed if it was closed before April 17, 2012. Of the 100 large-breach cases, we identified 69 cases that OCR closed, and 31 cases that were open at the time of our review. We calculated the number of covered entities involved in the 69 closed large-breach cases and the number of individuals affected by these breaches. Our estimates of the closed and open large-breach cases apply to our population of 264 large-breach cases that were reported to OCR during the period of September 23, 2009, to March 31, 2011.

We focused our analysis on the closed large-breach cases. Except where noted, we project our estimates to the subpopulations of (1) closed large-breach cases and (2) closed large-breach cases in which OCR made determinations of noncompliance.

We identified how OCR resolved the 69 closed large-breach cases. We categorized each of these closed large-breach cases as either (1) cases in which OCR made a determination of no violation with the HIPAA standards (i.e., OCR did not identify a violation or the evidence was insufficient to make a determination of a violation), or (2) cases in which OCR made a determination of noncompliance with at least one HIPAA standard. We put five closed cases in the first category. These are cases in which OCR determined that there was no evidence to indicate that the covered entity violated the HIPAA standards. We put 64 closed cases in the second category. These are cases in which OCR determined that the covered entity should take corrective action to address at least one of the HIPAA standards. We estimated the percentage of all closed large-breach cases in which OCR made determinations of no violation or noncompliance. Our estimates related to these 69 closed large-breach cases apply to a subpopulation of about 182 closed large-breach cases that covered entities reported to OCR during the period of September 23, 2009, to March 31, 2011.

We further analyzed the 64 closed large-breach cases in which OCR determined that covered entities were noncompliant with the HIPAA standards. We identified the most common type of noncompliance and describe corrective action taken by covered entities. Additionally, we reviewed the 64 closed large-breach cases to identify whether OCR had complete or incomplete documentation of corrective action in PIMS. We considered a case to have either (1) complete documentation (if PIMS had evidence that the covered entity took corrective action to address each of the HIPAA standards) or (2) incomplete documentation (if there was no evidence in PIMS to demonstrate that the covered entity took all corrective action). We estimated the percentage of cases that had complete or incomplete documentation of corrective action. This estimate applies to

a subpopulation of about 169 closed large-breach cases in which OCR determined that covered entities were noncompliant.

We determined that our population of 264 large-breach cases consisted of 247 unique covered entities. We identified similarly named covered entities (e.g., "ABC Company, Inc." and "ABC Co., Inc.") and made case-by-case determinations—on the basis of the available case information—as to whether they were the same covered entity or different ones. Using this approach, we counted the number of covered entities that had reported other large breaches to OCR.

Review of Small Breaches. We requested from OCR a list of all small breaches that covered entities reported to OCR during the period of September 23, 2009, to March 31, 2011. We received a list from OCR of 30,284 small breaches. We selected a simple random sample of 150 small breaches from this population, and requested that OCR provide us with all data (e.g., covered entity's name, estimated number of individuals affected by the breach, type of breach, and corrective action taken by the covered entity in response to the breach) for each of the small breaches. We reviewed the 150 small breaches that covered entities reported to OCR to determine whether OCR investigated them. We estimated the percentage of all small breaches investigated by OCR and project this estimate to our population of small breaches.

We determined that our sample of 150 small breaches consisted of 106 unique covered entities. As with the large breaches, we identified similarly named covered entities (e.g., "ABC Company, Inc." and "ABC Co., Inc.") and made case-by-case determinations on the basis of the available case information as to whether they were the same covered entity or different covered entities. Using this approach, we counted the number of covered entities that reported more than one small breach to OCR. We do not project our estimate of unique covered entities that reported small breaches to OCR during the period of September 23, 2009, to March 31, 2011.

Survey of OCR Staff. We administered an electronic survey to all 83 OCR staff who worked on breach cases to determine how they investigated these cases.[38] We had a 100-percent response rate. Of the 83 OCR staff, 61 indicated that they worked on large-breach cases during the period of September 23, 2009, to March 31, 2011, and 52 indicated that they worked

[38] We use the term "OCR staff" to include positions such as investigators, program staff assistants, interns, regional managers, and contractors who conducted preliminary reviews, assigned cases, contacted the covered entity or complainant, collected or reviewed documents, and/or reviewed case determinations.

on small-breach cases during this period.[39] For each group, we calculated the percentage of OCR staff who reported that they (1) always checked, (2) usually or sometimes checked, or (3) rarely or never checked whether covered entities had previously been investigated. We described OCR staff's explanations of why they rarely or never checked.

Interviews with OCR Officials and Review of OCR Documents. We interviewed OCR officials to learn how OCR oversees covered entities that reported breaches of PHI. We asked these officials how breach cases are investigated and how OCR staff use PIMS during their investigations.

We requested from OCR headquarters and regional offices all policies and procedures for investigating breach cases. We reviewed these policies and procedures to understand how OCR staff investigate breach cases and how they ensure that covered entities take corrective action.

Survey of Part B Providers. We selected a simple random sample of 150 Part B providers from the population of 913,235 Part B providers that submitted at least 1 Medicare claim in 2011. We used the National Claims History file to select a representative sample of Part B providers. This file had the most complete and recent Medicare claims data available at the time of our data request.

We surveyed the Part B providers to determine the extent to which they addressed three selected breach administrative standards. We administered an electronic survey to 150 Part B providers and obtained 132 responses, an 88-percent response rate. We project our estimates to 88 percent of our population, which is about 803,647 Part B providers that submitted at least 1 Medicare claim in 2011. Our 12-percent nonresponse rate consisted of Part B providers that either did not respond to the survey or did not receive the survey as a result of incomplete or inaccurate contact information.

We asked the 132 Part B providers whether they had addressed three selected breach administrative standards that require them to have: (1) established a sanctions policy for staff; (2) provided some or all staff with training on the covered entity's policies and procedures with respect to PHI;[40] and (3) implemented policies and procedures. We considered a Part B provider to have addressed the three standards if the provider submitted documents to demonstrate that it had a sanctions policy, provided training, and implemented policies and procedures.

[39] The numbers of OCR staff who indicated that they worked on large-breach cases and small-breach cases during the period of September 23, 2009, to March 31, 2011, are not mutually exclusive, as OCR staff worked on one or both types of breach cases.

[40] Although the standard requires covered entities to train *all* staff, we surveyed Part B providers to see whether they trained some or all staff. 45 CFR § 164.530(b)(1).

We reviewed documents to determine whether they addressed all three selected breach administrative standards. We estimated the percentages of Part B providers that (1) addressed *all* three selected breach administrative standards, (2) addressed *each* of the three breach administrative standards, (3) expressed interested in learning more about OCR and about the Breach Notification Rule, and (4) responded that they were unfamiliar with OCR's jurisdiction over the Breach Notification Rule.

APPENDIX B

Table B-1: Point Estimates and Confidence Intervals for the Subpopulation of Large Breach Cases

Estimate Description	Sample Size	Point Estimate (Number of Cases)	95-Percent Confidence Interval
Subpopulation of closed large-breach cases	100 large-breach cases	182	163–201
Subpopulation of closed large-breach cases in which OCR made determinations of noncompliance		169	149–189

Source: OIG analysis of data from OCR large-breach cases, 2015.

Table B-2: Point Estimates and Confidence Intervals for Large Breaches and Small Breaches

Estimate Description	Sample Size	Point Estimate	95-Percent Confidence Interval
Large breaches investigated during the period of September 23, 2009, to March 31, 2011	100 large breaches	100%	97.0%–100%
Large-breach cases that were closed prior to April 17, 2012	100 large-breach cases	69.0%	59.8%–78.2%
Large-breach cases that were open as of April 17, 2012		31.0%	21.8%–40.2%
Closed large-breach cases in which OCR determined covered entities were noncompliant with at least one HIPAA standard	69 closed large-breach cases	92.8%	83.9%–97.6%
Closed large-breach cases in which OCR determined covered entities to be compliant with the HIPAA standards		5.8%	1.6%–14.2%
Closed large-breach cases for which OCR did not have any investigation information		1.4%	0%–7.8%
Closed large-breach cases in which OCR determined covered entities to be noncompliant and did not have complete documentation of corrective action in PIMS	64 closed large-breach cases in which OCR determined covered entities to be noncompliant	23.4%	13.8%–35.7%
Closed large-breach cases in which OCR determined covered entities to be noncompliant and had complete documentation of corrective action in PIMS		76.6%	64.3%–86.2%
Small breaches investigated by OCR during the period of September 23, 2009, to March 31, 2011	150 small breaches	0%	0%–2.4%

Source: OIG analysis of data from OCR large and small-breach cases, 2015.

APPENDIX B

Table B-3: Point Estimate and Confidence Interval for the Subpopulation of Part B Providers

Estimate Description	Sample Size	Point Estimate (Number of Part B Providers)	95-Percent Confidence Interval
Subpopulation of Part B providers that responded to the survey	150 Part B providers	803,647	755,610–851,684

Source: OIG analysis of data from the Part B Provider survey, 2015.

Table B-4: Point Estimates and Confidence Intervals for the Part B Provider Survey

Estimate Description	Sample Size	Point Estimate	95-Percent Confidence Interval
Part B providers that did not address all three selected breach administrative standards	132 Part B providers	26.5%	18.9%–34.1%
Part B providers that addressed all three selected breach administrative standards		73.5%	65.9%–81.1%
Part B providers that had not established a sanctions policy for staff		23.5%	16.5%–31.6%
Part B providers that had not provided some or all staff with training on their organization's policies and procedures with respect to PHI		21.2%	14.6%–29.2%
Part B providers that had not implemented PHI policies and procedures that complied with the Breach Notification Rule		17.4%	11.4%–25%
Part B providers that expressed interest in learning more about OCR and the Breach Notification Rule		62.1%	53.7%–70.5%
Part B providers that reported that they were unfamiliar with OCR's jurisdiction over the Breach Notification Rule		34.8%	26.6%–43.1%

Source: OIG analysis of data from the Part B Provider survey, 2015.

APPENDIX C

Agency Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Director
Office for Civil Rights
Washington, D.C. 20201

DATE: September 23, 2015

TO: Daniel Levinson
Inspector General

FROM: Jocelyn Samuels
Director
Office for Civil Rights

SUBJECT: Office of Inspector General (OIG) Draft Report: "OCR Should Strengthen its Follow Up on Covered Entity Reported Breaches of Patient Health Information" (OEI-09-10-00511)

The Office for Civil Rights (OCR) appreciates the opportunity to review and comment on the subject OIG draft report. The objectives of this report are to assess OCR's oversight of covered entities' compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act Breach Notification Rule, and to determine the extent to which Medicare Part B providers complied with three selected requirements of the Breach Notification Rule. OIG's assessment of OCR's oversight is based on its review of a sample of cases involving breaches reported to OCR between September 23, 2009 (the effective date of the Rule), and March 31, 2011.

OCR is committed to ensuring that covered entities and their business associates comply with the requirements of the Breach Notification Rule, which serve to increase public transparency of breaches and accountability of covered entities and business associates to secure patient data. OCR exercises its oversight responsibilities by providing technical assistance and requiring corrective action, where appropriate, to ensure that covered entities and business associates are implementing appropriate safeguards to prevent breaches of protected health information, as well as taking appropriate remedial action and making the required notifications when a reportable incident does occur. OCR reviews breach notification reports and initiates investigations into all breaches involving 500 or more individuals, as well as into a number of breaches involving fewer than 500 individuals. In addition, OCR provides guidance and educational materials and actively seeks opportunities to engage with regulated entities to improve awareness of, and compliance with, the Breach Notification Rule.

We appreciate OIG's efforts to work with OCR to ensure that covered entities and their business associates are aware of the requirements of the Breach Notification Rule and to ensure effective and efficient enforcement. We believe that our breach notification program has been successful to date in advancing the goals of the HITECH Act but we always welcome ideas for further improvements, which we consider as resources permit. OCR faces significant resource constraints since taking on additional responsibilities under the law without additional budgetary resources. Our specific response to each of the OIG recommendations follows.

OIG Recommendation

The OIG recommends that OCR enter all small breach case information into PIMS or a searchable database linked to PIMS.

OCR Response

OCR concurs with this recommendation. OCR undertook a major update to its breach portal and electronic document management and investigations tracking system, called the Program Information Management System (PIMS), which it implemented in January of this year. To address this issue, OCR completed several PIMS enhancements as part of that update that allow for investigative and other staff nationally to search and track all breach notifications and create reports. In addition, the enhancements capture small breach notifications and their associated data elements and case information within PIMS for more detailed reporting and analysis for investigatory purposes.

OIG Recommendation

The OIG recommends that OCR maintain complete documentation in PIMS of corrective actions taken by covered entities.

OCR Response

OCR concurs with this recommendation. While OCR requires that its investigators maintain complete documentation of all corrective actions taken by HIPAA covered entities and business associates as a result of an investigation by OCR, we realize that there may be instances where complete documentation is not uploaded into PIMS. OCR will work to ensure that all investigators working on cases involving the HIPAA Rules understand the appropriate procedures for maintaining documentation of corrective actions in PIMS. Additionally, OCR will explore OIG's suggestion regarding development of a tool in PIMS to track required documentation.

OIG Recommendation

The OIG recommends that OCR develop an efficient method in PIMS to search for covered entities that reported prior breaches.

OCR Response

OCR concurs with this recommendation. As mentioned in the response to the previous recommendation, OCR completed several enhancements to PIMS that have increased the functionality with regard to the ability to search and track breach reports. OCR has also created a standardized method to search and track breach reports and determine whether covered entities or business associates reported prior breaches.

OIG Recommendation

The OIG recommends that OCR develop a policy requiring OCR staff to consistently check for prior breaches.

OCR Response

OCR concurs with this recommendation. While many investigators do regularly check PIMS for prior breaches, or rely on administrative staff to do so, we recognize the importance of a standard policy requiring such a practice. Now that OCR has completed a multitude of enhancements to PIMS, we will develop internal guidance, as well as a standardized process, that will require all OCR investigators to consistently check for prior breaches submitted by covered entities and their business associates when initiating an investigation.

OIG Recommendation

The OIG recommends that OCR continue to expand outreach and education efforts.

OCR Response

OCR concurs with this recommendation. To fulfill the HITECH Act's mandate to develop and maintain a multi-faceted national education program, and to address compliance deficiencies in the regulated community identified by its compliance and enforcement program, OCR significantly amplified its public outreach and education campaign beginning in 2010 and continuing to today, with the goal of increasing compliance with the HIPAA Rules across the health care industry and consumer awareness. These efforts have included: (1) launching a YouTube channel that features videos for regulated entities and consumers; (2) establishing a Medscape "Resource Center," which contains on-line HIPAA training modules that offer free Continuing Medical Education (CME) credits for physicians and Continuing Education (CE) credits for health care professionals; (3) developing various guidance documents and related resources, including, in coordination with the Office of the National Coordinator for Health Information Technology, guidance addressing mobile device security and a tool to help small providers perform risk analyses; and (4) participating in speaking events and webinars on the breach notification and other requirements under the HIPAA Rules that collectively reach thousands of stakeholders annually. OCR also partnered with the Centers for Medicare and Medicaid Services (CMS) to provide education specifically geared toward Medicare Part B providers regarding their obligations under the HIPAA Rules. These resources included an informational Medlearn™ Matters fact sheet, on-line educational modules available for free CME and CE credits, and MLN Connects™ National Provider conference calls held by OCR for the Medicare provider and supplier community. HIPAA guidance documents and related resources are available on the OCR web site at http://www.hhs.gov/ocr/privacy/. OCR continues to develop additional guidance materials, speak at national conferences and educational events, and expand the tools available to the regulated community to improve compliance with the HIPAA Rules.

OCR thanks OIG for its work on this issue and looks forward to working with OIG in the future.

ACKNOWLEDGMENTS

This report was prepared under the direction of Blaine Collins, Regional Inspector General for Evaluation and Inspections in the San Francisco regional office and Michael Henry, Deputy Regional Inspector General.

Abby Amoroso served as the team leader for this study, and Christina Lester served as the lead analyst. Other Office of Evaluation and Inspections staff from the San Francisco regional office who contributed to the study include Timothy Brady, Joyce Greenleaf, Camille Harper, and Linda Min. Central office staff who provided support include Heather Barton, Kevin Farber, Robert Gibbons, Christine Moritz, and Sherri Weinstein.

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95452, 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 individuals 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 individuals. 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.