Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

OCR SHOULD STRENGTHEN ITS OVERSIGHT OF COVERED ENTITIES' COMPLIANCE WITH THE HIPAA PRIVACY STANDARDS

Suzanne Murrin
Deputy Inspector General for Evaluation and Inspections

September 2015
OEI-09-10-00510

EXECUTIVE SUMMARY: OCR SHOULD STRENGTHEN ITS OVERSIGHT OF COVERED ENTITIES' COMPLIANCE WITH THE HIPAA PRIVACY STANDARDS
OEI-09-10-00510

WHY WE DID THIS STUDY

Covered entities such as doctors, pharmacies, and health insurance companies that do not adequately safeguard patients' protected health information (PHI) could expose patients to an invasion of privacy, fraud, identity theft, and/or other harm. PHI includes identifying information like a patient's name, test results, medical condition, prescriptions, or treatment history. The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) established standards for sharing, using, and disclosing individuals' PHI and charges the Office for Civil Rights (OCR) with enforcing covered entities' compliance with the HIPAA privacy standards.

HOW WE DID THIS STUDY

To assess OCR's oversight of covered entities' compliance with the Privacy Rule, we (1) reviewed a statistical sample of privacy cases that OCR investigated 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 five selected privacy standards.

WHAT WE FOUND

OCR should strengthen its oversight of covered entities' compliance with the Privacy Rule. OCR's oversight is primarily reactive; it investigates possible noncompliance primarily in response to complaints. OCR has not fully implemented the required audit program to proactively assess possible noncompliance from covered entities. In about half of the closed privacy cases, OCR determined that covered entities were noncompliant with at least one privacy standard. In most cases in which OCR made determinations of noncompliance, it requested corrective action from the covered entities. OCR documented corrective action in its case-tracking system for most of these cases; however, OCR did not have complete documentation of corrective actions taken by the covered entities in 26 percent of closed privacy cases. Although 71 percent of OCR staff at least sometimes checked whether covered entities had been previously investigated, some 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 responses to our survey of Medicare Part B providers and documents that they provided, most providers addressed all five selected privacy standards, but 27 percent did not. These Part B providers may not be adequately safeguarding PHI.

WHAT WE RECOMMEND

OCR should (1) fully implement a permanent audit program; (2) maintain complete documentation of corrective action; (3) develop an efficient method in its case-tracking system to search for and track covered entities; (4) develop a policy requiring OCR staff to check whether covered entities have been previously investigated; 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' compliance with the standards established by the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA).
2. To determine the extent to which Medicare Part B providers addressed five selected privacy standards.

BACKGROUND

OCR is responsible for overseeing covered entities' compliance with the Privacy Rule, which provides Federal safeguards to maintain the privacy of individuals' protected health information (PHI).[1] PHI is individually identifiable health information in any form, including electronic, oral, or paper.[2] Examples of PHI include an individual's name, Medicare number, or medical history. A failure to safeguard PHI may lead to identity theft, inappropriate billing, and/or other financial or reputational harm to individuals whose PHI has been compromised. As of September 2015, OCR had received more than 120,000 complaints regarding alleged privacy violations since the Privacy Rule went into effect in April 2003.[3]

Covered Entities

The Privacy Rule applies to three types of covered entities.[4] 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.[5] Health plans are individual or group plans that provide or pay for medical care, and include governmental plans, such as Medicare and Medicaid.[6] Health care clearinghouses include businesses that process or help to process health information received from another covered entity, as well as businesses

[1] 45 CFR pt. 164, subpt. E. The Privacy Rule is one of three HIPAA rules that aim to safeguard PHI. OCR is also responsible for overseeing two other HIPAA rules—the Security Rule and Breach Notification Rule. 45 CFR 164, subpts. C and D.

[2] 45 CFR § 160.103.

[3] OCR, *Privacy Rule Enforcement Highlights*. Accessed at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html on September 23, 2015.

[4] The Privacy 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 a covered entity, or a person or entity that provides services to a covered entity. 45 CFR § 160.103.

[5] 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).

[6] 45 CFR § 160.103.

that receive HIPAA-covered transactions from another covered entity.[7] 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.[8]

Privacy Rule Standards for Covered Entities

Covered entities were required to comply with the Privacy Rule standards (privacy standards) by April 14, 2003.[9] In general, the privacy 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.[10]

OCR Oversight of Covered Entities

OCR uses several mechanisms to oversee covered entities' compliance with the privacy standards. It may investigate covered entities in response to complaints, tips, or media reports. OCR may also proactively conduct audits of covered entities to assess their compliance efforts. The Health Information Technology for Economic and Clinical Health Act (HITECH Act) required OCR to provide for such audits, effective February 2010.[11] Also, the HITECH Act requires OCR to offer guidance and education to covered entities on their rights and responsibilities related to the privacy standards.[12]

OCR Investigation of Privacy Cases. OCR has discretion on how to investigate privacy cases, which includes, but is not limited to, conducting interviews, document reviews, and onsite visits.[13, 14] It may check whether a covered entity has been previously investigated for other privacy-related complaints. 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 privacy standards.[15]

OCR Resolutions of Privacy Cases. After OCR investigates, it may resolve a privacy case with a determination of no violation, or, if there is

[7] 45 CFR § 160.103.

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

[9] 45 CFR § 164.534.

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

[11] HITECH Act, §§ 13411 and 13423.

[12] HITECH Act, § 13403.

[13] 45 CFR § 160.310(c)(1).

[14] In their investigations of privacy cases, OCR staff may also investigate standards related to the Security Rule and Breach Notification Rule.

[15] 45 CFR § 160.304(b).

an indication of noncompliance, by requesting that the covered entity take corrective action.[16] A determination of no violation means that OCR did not identify a violation with 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 standard. Corrective action can include retraining staff on appropriate disclosures of PHI, revising policies, and implementing safeguards to protect PHI. Because OCR may investigate more than one standard per privacy case, a single investigation can result in multiple determinations.

OCR may also resolve a privacy case by entering into a resolution agreement with the covered entity.[17] 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.[18, 19] In determining a CMP amount, OCR may consider, among other factors, a covered entity's history of noncompliance with the privacy standards.[20]

If OCR makes a determination that the covered entity did not violate the privacy 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.

OCR Program Information Management System

OCR staff use the Program Information Management System (PIMS) to electronically document their investigation of privacy cases.[21] OCR staff use this case-tracking system to record (1) actions taken by OCR staff and by the covered entity, (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 OCR staff maintain in PIMS documentation of the corrective action taken by a

[16] 45 CFR § 160.312.

[17] 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.

[18] 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.

[19] 45 CFR pt. 160, subpt. D.

[20] 45 CFR § 160.408.

[21] 67 Fed. Reg. 57011–57012 (Sept. 6, 2002).

covered entity. OCR staff can also use PIMS to search for previous investigations of covered entities.

Related OIG Work

This report is part of 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.[22] In a November 2013 report, OIG found that OCR did not meet all Federal requirements in its oversight and enforcement of the HIPAA Security Rule.[23] Additionally, OIG is issuing a companion report on OCR's followup regarding covered entities that reported breaches of patient health information.[24]

METHODOLOGY

Data Collection and Analysis

To assess OCR's oversight of covered entities' compliance with the privacy standards, we (1) reviewed a statistical sample of privacy cases; (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 five selected privacy standards, we surveyed and collected documents from a statistical sample of Part B providers. See 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 Privacy Cases. We reviewed privacy cases to determine how OCR resolved them, and to determine the extent to which OCR documented covered entities' corrective action in PIMS. We selected a simple random sample of 150 privacy cases from a population of 7,080 cases that OCR investigated during the period of September 23, 2009, to March 31, 2011. We focused our analysis on the privacy cases that had been closed. Except where noted, we project our

[22] 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 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 24, 2015.

[23] 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 24, 2015.

[24] OIG, *OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities*, OEI-09-10-00511.

estimates to the subpopulations of (1) closed privacy cases, (2) closed privacy cases in which OCR made determinations of noncompliance, and (3) closed privacy cases in which OCR requested corrective action.

Survey of OCR Staff. We surveyed all 133 OCR staff who worked on privacy cases and asked how they investigated these cases. We had a 100-percent response rate.

Interviews With OCR Officials and Review of OCR Documents. We interviewed OCR officials to understand how OCR investigates privacy 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 the five selected privacy standards that require them to:

(1) have established a sanctions policy for staff;

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

(3) maintain a Notice of Privacy Practices;

(4) have designated a privacy official; and

(5) provide a complaint process for individuals.[25]

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 privacy cases is limited to the information provided by OCR. We did not contact covered entities to verify information regarding privacy cases, such as corrective action that was recorded in PIMS. We did not determine whether each privacy case was appropriately resolved by OCR staff. We did not examine the determinations reached by OCR or the corrective action taken in previous privacy cases that involved the same covered entities. Our analysis of the OCR staff survey is from

[25] These five privacy standards are located at 45 CFR § 164.530 and 45 CFR § 164.520.

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.

FINDINGS

OCR investigated possible noncompliance with the privacy standards primarily in response to complaints; OCR has not fully implemented the required audit program to proactively identify possible noncompliance from covered entities

OCR oversees covered entities' compliance with the privacy standards primarily by responding to complaints, tips, or media reports of possible noncompliance. In 98 percent of all closed privacy cases, OCR initiated its investigations because of complaints. OCR investigated the remaining 2 percent in response to tips or media reports.

Although the HITECH Act requirement for audits was effective as of February 2010, OCR has not fully implemented an audit program to proactively assess covered entities' compliance with the privacy standards. As of July 2015, OCR had made progress towards meeting the requirement by launching a pilot audit program and evaluating the program's results.[26] However, OCR had not announced when it will begin its permanent audit program. Without fully implementing such a program, OCR cannot proactively identify covered entities that are noncompliant with the privacy standards.

In about half of the closed privacy cases, OCR determined that covered entities were noncompliant with at least one privacy standard

OCR determined that covered entities were noncompliant with at least one privacy standard in 54 percent of closed privacy cases.[27] A determination of noncompliance may indicate that covered entities lack appropriate safeguards to protect health information. Among the closed privacy cases in our sample in which OCR made determinations of noncompliance, the two most common types of noncompliance were related to the standard on restricting uses and disclosures of PHI and the standard on implementing

[26] OCR, *OCR Audits of HIPAA Privacy, Security, and Breach Notification, Phase 2*. Accessed at http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2014/tue/710print2color.pdf on June 3, 2015.

[27] In 44 percent of the closed privacy cases, OCR determined that covered entities did not violate the privacy standards (i.e., OCR did not identify a violation or the evidence was insufficient to make a determination of a violation). The remaining 2 percent of closed privacy cases did not have any information as to how OCR resolved the cases.

safeguards.[28] The most frequently represented covered entities among these cases were hospitals and individual providers.

OCR requested that covered entities take corrective action in 85 percent of the privacy cases in which it determined that covered entities were noncompliant. Among these cases that were in our sample, corrective actions included, for example, developing or revising privacy policies, implementing sanctions for staff who did not comply with the privacy policies, and training employees on the organization's privacy policies. For the remaining 15 percent of privacy cases, OCR provided technical assistance and did not request that the covered entities take corrective action. 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 privacy cases that were in our sample.

OCR documented corrective action for almost three-quarters of privacy cases in which it requested such actions from covered entities; however, 26 percent of cases had incomplete documentation

Of privacy cases in which OCR requested that covered entities take corrective action, 26 percent lacked complete documentation in PIMS of such actions. For the remaining 74 percent, OCR had complete documentation of corrective action in PIMS. Without complete documentation, OCR cannot verify whether covered entities took corrective action to address noncompliance with the privacy standards.

Seventy-one percent of OCR staff at least sometimes checked whether covered entities had been previously investigated; however, 29 percent rarely or never did so

Although OCR staff have the discretion to check whether a covered entity has been previously investigated, 29 percent of OCR staff reported that they rarely or never made such checks. The reasons they gave for rarely or never checking varied, including that they relied on other staff to do such checks, that they believed previous investigations of the covered entity did not impact the current case, and/or that they lacked an efficient way to search for covered entities in PIMS. However, 57 percent of OCR staff reported that they usually or sometimes checked, and 14 percent

[28] The privacy standard on restricting uses and disclosures of PHI may address, for example, the disclosure of a patient's PHI to an unauthorized individual. 45 CFR § 164.502. The privacy standard on implementing safeguards may address, for example, the use of facility access controls (e.g., key locks on facilities, attended entrances, keyed physical access cards). 45 CFR § 164.530(c)(1).

reported that they always checked whether a covered entity had been previously investigated.

In our sample, we identified 44 covered entities that OCR investigated more than once. OCR investigated 23 of these covered entities at least 5 times each. Without checking for a history of investigations, OCR cannot identify covered 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 they are 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 staff's ability to identify covered entities that had been previously investigated. 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 search for all possible variations of a covered entity's name to generate a comprehensive history of previous investigations and their resolutions. 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 it can use to determine the amount of a CMP.

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

According to our analysis of responses to our Part B provider survey and the supporting documents that they provided, 27 percent of providers did not address all five selected privacy standards. By not addressing these standards, Part B providers could be placing PHI at risk of misuse or inappropriate disclosure. Because OCR's primary oversight activity is responding to complaints, it may not be aware of Part B providers—or covered entities, in general—that do not address the privacy standards. See Table 1 for the percentage of Part B providers that did not address each of the selected privacy standards.

Table 1: Percentage of Part B providers that did not address each of the selected privacy standards

Selected privacy standard	Percentage of Part B providers that did not address the standard
Established a sanctions policy for staff	24%
Provided some or all staff with training on the covered entity's policies and procedures with respect to PHI	20%
Maintained a Notice of Privacy Practices	16%
Designated a privacy official	11%
Provided a complaint process for individuals	9%

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

The remaining 73 percent of Part B providers addressed all five selected privacy standards. As examples of how they addressed the selected privacy standards, Part B providers submitted to OIG their sanctions policies and training materials on the standards, and provided the names and phone numbers of their designated privacy officials.

Fifty-five percent of Part B providers expressed interest in learning more about OCR and the Privacy Rule. Some Part B providers were interested in receiving updates from OCR regarding the privacy standards, learning more about the privacy standards to ensure compliance, receiving guidance on how to implement best practices for safeguarding PHI, and having access to education materials and training tools. Twenty-seven percent of Part B providers reported that they were unfamiliar with OCR's jurisdiction over the Privacy 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 Privacy Rule.

CONCLUSION AND RECOMMENDATIONS

OCR should strengthen its oversight of covered entities' compliance with the Privacy Rule. OCR's oversight is primarily reactive; it investigates cases in response to complaints, tips, or media reports. It has not yet fully implemented the required audit program to proactively identify possible noncompliance from covered entities. Our survey of Part B providers identified that most providers addressed five selected privacy standards; however, 27 percent did not. Because OCR relies primarily on complaints, it may not know about these Part B providers or other covered entities that may not be complying with the Privacy Rule. Covered entities that do not adequately safeguard PHI could expose individuals to identity theft, and/or other financial or reputational harm.

OCR could improve its current investigation process. OCR determined covered entities were noncompliant with the privacy standards in about half of the closed privacy cases. Most of these cases warranted corrective action. Although OCR documented corrective action for almost three-quarters of those privacy cases, 26 percent of the cases did not have complete documentation of such actions. Further, while 71 percent of OCR staff reported that they at least sometimes check whether covered entities had histories of investigations, 29 percent said that they rarely or never do so. If OCR staff wanted to check, they may face challenges because OCR does not have a standard way to enter covered entities' names in PIMS, its case-tracking system.

We recommend that OCR:

Fully implement a permanent audit program

Although OCR has made progress towards implementing the required audit program, it should fully implement a permanent proactive audit program to assess covered entities' compliance with the privacy standards. OCR should enter audit and investigation information into a searchable database linked to PIMS or further develop PIMS to effectively track covered entities that OCR audits and investigates. The proactive audits will supplement OCR's current approach of investigating privacy cases in response to complaints, tips, or media reports.

Maintain complete documentation in PIMS of corrective action

OCR should maintain complete documentation in PIMS of corrective action. OCR should develop a process in PIMS—e.g., a checklist—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' histories of being investigated

To effectively record, track, and search for information about investigations of covered entities, OCR could enter unique provider identifiers in PIMS, such as the National Provider Identifier or Employer Identification Number.[29] 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 have been previously investigated

If OCR staff check whether a covered entity has been previously investigated, they could identify those that may have systemic problems in safeguarding PHI. Covered entities that are currently being investigated and have a history of noncompliance may not be addressing systemic gaps in safeguarding individuals' PHI. For covered entities that have a history of noncompliance, OCR could also conduct onsite visits, initiate compliance reviews, or perform audits. In addition, OCR could consider a covered entity's history of noncompliance in determining an appropriate resolution, such as using 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 privacy standards, OCR could target certain industry and professional health care associations to educate covered entities about OCR and the privacy 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 changes to the privacy standards; (3) continue to provide resources, such as Web seminars on compliance; and (4) assess the impact of its outreach and education efforts to focus on those determined to be effective. OCR could also work with CMS—the agency that oversees Medicare—to increase Part B providers' compliance with the Privacy Rule.

[29] HIPAA requires employers to have standard national numbers that identify them on general transactions. CMS selected the Employer Identification Number as the identifier for employers, effective July 2002.

AGENCY COMMENTS

OCR concurred with all five of OIG's recommendations and described its activities to address our recommendations. As of September 2015, OCR reported that its case-tracking system has been upgraded, which enables OCR staff 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. Additionally, 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. Further, OCR described the results of its pilot audit program and reported that it plans to start the second phase of its audit program in 2016.

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

APPENDIX A

Detailed Methodology

Scope

We reviewed a sample of privacy cases investigated by OCR during the period of September 23, 2009, to March 31, 2011. Our review focused on privacy cases that OCR had closed, cases in which OCR made determinations of noncompliance, and cases in which OCR requested corrective action.

We surveyed and requested documents from a sample of Part B providers that submitted at least one Medicare claim in 2011.[30] We selected five privacy standards for which we could collect from providers documentation showing that they addressed the standards.

Data Collection and Analysis

We used four data sources for our evaluation: (1) a review of OCR privacy cases; (2) a survey of OCR staff; (3) interviews with OCR officials and a review of OCR's policies and procedures for investigating privacy cases; and (4) a survey of Part B providers.

Review of OCR Privacy Cases. We requested from OCR a list of all privacy cases that OCR staff investigated during the period of September 23, 2009, to March 31, 2011. We received from OCR a list of 7,080 privacy cases. We selected a simple random sample of 150 privacy cases from this population. For each of the 150 cases, we requested that OCR provide us with all related data—e.g., actions that OCR and the covered entity took, evidence gathered during the investigation, OCR's determinations, and any supporting documentation from the covered entity.

We categorized each of the 150 privacy cases as open or closed. We considered a privacy case to be open if it was open as of April 17, 2012, the date on which we received the privacy case data from OCR. We considered a privacy case to be closed if it had been closed before April 17, 2012. Of the 150 privacy cases, we identified 127 privacy cases that OCR had investigated and closed, and 23 that were open at the time of our review.

We focused our analysis on the closed privacy cases. Except where noted, we project our estimates to the subpopulations of (1) closed privacy cases,

[30] 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.

(2) closed privacy cases in which OCR made determinations of noncompliance, and (3) closed privacy cases in which OCR requested corrective action.

We reviewed the 127 closed privacy cases to determine what prompted OCR's investigations. We estimated the percentage of all closed privacy cases that were initiated in response to complaints filed by individuals or in response to tips or media reports. Our estimates related to the 127 closed privacy cases apply to a subpopulation of about 5,994 closed privacy cases that OCR investigated during the period of September 23, 2009, to March 31, 2011.

Additionally, we categorized the 127 privacy cases as cases in which OCR (1) made a determination of no violation with the privacy standards (i.e., OCR did not identify a violation or the evidence was insufficient to make a determination of a violation), (2) made a determination of noncompliance with at least one standard, or (3) made no final determination. We put 56 closed privacy 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 privacy standards. We put 68 closed privacy 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 privacy standard or if the covered entity received technical assistance from OCR. The remaining three cases were closed, but OCR did not have any final determination information. We then estimated the percentages of all closed privacy cases in the three categories.

We conducted additional analysis on the 68 closed privacy cases in which OCR determined that covered entities were noncompliant with the standards. Our estimates related to these 68 cases apply to a subpopulation of about 3,210 closed privacy cases in which OCR determined that covered entities were noncompliant.

Among the 68 closed privacy cases in which OCR determined that covered entities were noncompliant, we identified the privacy standards for which OCR most often determined that covered entities were noncompliant and requested corrective action. We also identified the two most common types of standards with which covered entities did not comply and the most frequently represented types of covered entities that OCR determined were noncompliant. We identified 58 closed privacy cases in which OCR requested that the covered entities take corrective action and 10 cases in which OCR provided technical assistance. We estimated the percentage of closed privacy cases in which OCR requested that the covered entities take corrective action, and the percentage in

which it provided technical assistance to the covered entities and did not request that they take corrective action.

We further analyzed the 58 closed privacy cases in which OCR requested corrective action to determine whether OCR had complete or incomplete documentation in PIMS of such actions. We considered a case to have complete documentation if PIMS had evidence that the covered entity took corrective action to address each privacy standard. We considered a case to have incomplete documentation if there was no evidence in PIMS to demonstrate that the covered entity took all corrective action. We estimated the respective percentage of cases that had complete or incomplete documentation of corrective action. This estimate applies to a subpopulation of about 2,738 closed privacy cases in which OCR made determinations of noncompliance and requested corrective action.

We determined that our sample of 150 privacy cases consisted of 133 unique covered entities. We requested from OCR the information on the number of times each covered entity had been previously investigated. We considered similarly named covered entities (e.g., "ABC Company, Inc." and "ABC Co., Inc.") to be different covered entities because we could not verify their information. Using this approach, we counted the number of covered entities that OCR reported as having been investigated more than once. We do not project our estimate of unique covered entities to the population of privacy cases investigated by OCR during the period of September 23, 2009, to March 31, 2011.

Survey of OCR Staff. We administered an electronic survey to all 133 OCR staff who worked on privacy cases to determine how they investigated these cases.[31] We had a 100-percent response rate. 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 been previously investigated. For OCR staff that reported rarely or never, we reviewed their responses as to why they rarely or never checked and we described their reasons.

Interviews With OCR Officials and Review of OCR Documents. We interviewed OCR officials to learn how OCR oversees covered entities' compliance with the privacy standards. We asked these officials how privacy cases are investigated and how OCR staff use PIMS during their investigations.

[31] 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.

We requested from OCR headquarters and regional offices all policies and procedures for investigating privacy cases. We reviewed these policies and procedures to understand how OCR staff investigate privacy 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 five selected privacy 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 the five privacy standards that require them to (1) have established a sanctions policy for staff; (2) have provided some or all staff with training on the covered entity's policies and procedures with respect to PHI;[32] (3) maintain a Notice of Privacy Practices; (4) have designated a privacy official; and (5) provide a complaint process for individuals. We considered a Part B provider to have addressed the first three standards if it submitted documents to demonstrate that it had a sanctions policy, that it provided training, and that it had a Notice of Privacy Practices. We considered a Part B provider to have addressed the fourth and fifth standards if it included in the survey a privacy official's name and phone number and described its complaint process or submitted documents explaining its complaint process.

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

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

APPENDIX B

Table B-1: Point Estimates and Confidence Intervals for the Subpopulations of Privacy Cases

Estimate Description	Sample Size	Point Estimate (Number of Cases)	95-Percent Confidence Interval
Subpopulation of closed privacy cases	150 privacy cases	5,994	5,586–6,403
Subpopulation of closed privacy cases in which OCR made determinations of noncompliance		3,210	2,645–3,774
Subpopulation of closed privacy cases in which OCR requested corrective action		2,738	2,185–3,290

Source: OIG analysis of data from OCR privacy cases, 2015.

Table B-2: Point Estimates and Confidence Intervals for the Privacy Cases

Estimate Description	Sample Size	Point Estimate	95-Percent Confidence Interval
Closed privacy cases initiated in response to complaints	127 closed privacy cases	98.4%	94.4%–99.8%
Closed privacy cases initiated in response to tips or media reports		1.6%	0.2%–5.6%
Closed privacy cases in which OCR made a determination of noncompliance with at least one standard		53.5%	44.8%–62.3%
Closed privacy cases in which OCR made a determination of no violation with the standards		44.1%	35.3%–52.8%
Closed privacy cases in which OCR made no final determination		2.4%	0.5%–6.7%
Closed privacy cases in which OCR determined that covered entities were noncompliant and requested that covered entities take corrective action	68 closed privacy cases in which OCR determined covered entities were noncompliant	85.3%	74.6%–92.7%
Closed privacy cases in which OCR determined that covered entities were noncompliant and provided technical assistance but did not request corrective action		14.7%	7.3%–25.4%
Closed privacy cases in which OCR requested corrective action and documentation of corrective action was incomplete	58 closed privacy cases in which OCR requested corrective action	25.9%	14.2%–37.5%
Closed privacy cases in which OCR requested corrective action and documentation of corrective action was complete		74.1%	62.5%–85.8%

Source: OIG analysis of data from OCR privacy 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 survey of Part B providers, 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 five selected privacy standards	132 Part B providers	27.3%	19.6%–35.0%
Part B providers that addressed all five selected privacy standards		72.7%	65.0%–80.4%
Part B providers that did not establish a sanctions policy for staff		23.5%	16.5%–31.6%
Part B providers that did not provide some or all staff with training on the covered entity's policies and procedures with respect to PHI		19.7%	13.3%–27.5%
Part B providers that did not maintain a Notice of Privacy Practices		15.9%	10.1%–23.3%
Part B providers that did not designate a privacy official		11.4%	6.5%–18.0%
Part B providers that did not provide a complaint process for individuals		9.1%	4.8%–15.3%
Part B providers that expressed interest in learning more about OCR and the Privacy Rule		54.5%	45.9%–63.2%
Part B providers that reported that they were unfamiliar with OCR's jurisdiction over the Privacy Rule		27.3%	19.6%–35.0%

Source: OIG analysis of data from survey of Part B providers, 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 R. Levinson
Inspector General

FROM: Jocelyn Samuels
Director
Office for Civil Rights

SUBJECT: Office of Inspector General (OIG) Draft Report: "OCR Should Strengthen its Oversight of Covered Entities' Compliance with the HIPAA Privacy Rule" (OEI-09-10-00510)

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 Insurance Portability and Accountability Act (HIPAA) Privacy Rule, and to determine the extent to which Medicare Part B Providers complied with five selected HIPAA Privacy Rule standards. OIG's assessment of OCR's oversight is based on its review of a sample of Privacy Rule cases investigated by OCR between September 23, 2009, and March 31, 2011.

As the office responsible for administration and enforcement of the HIPAA Privacy Rule, OCR is committed to ensuring strong privacy protections for individuals' identifiable health information and individual rights with respect to the information. OCR exercises its oversight responsibilities by providing technical assistance and requiring corrective action, where appropriate, to ensure covered entities and business associates are complying with their obligations under the Privacy Rule. 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 Privacy Rule.

We appreciate OIG's efforts to work with OCR to continue to ensure that covered entities and business associates understand their obligations under the Privacy Rule, and to ensure an effective and efficient Privacy Rule compliance and enforcement program. We believe that our Privacy Rule compliance and enforcement program has been successful to date in achieving strong privacy protections and rights for individuals 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 Health Information Technology for Economic and Clinical Health (HITECH) Act without additional budgetary resources. Our specific response to each of the OIG recommendations follows.

OIG Recommendation

The OIG recommends that OCR fully implement a permanent audit program.

OCR Response

OCR concurs with this recommendation, and we appreciate the acknowledgement of our progress in implementing a permanent audit program. A permanent program of periodic audits can provide new information about risks to, and weaknesses in the protection of, individually identifiable health information, and is an important outreach and compliance tool. An audit program can generate analytical tools and methods for entity self-evaluation, foster a culture of compliance throughout the health care sector, and serve as a foundation for enforcement action, where appropriate.

As required by the HITECH Act, OCR designed, tested, and evaluated an audit function to measure compliance with HIPAA privacy, security, and breach notification requirements by covered entities and their business associates. OCR finished field work for the pilot audit program in the first quarter of FY2013 and spent the balance of the year conducting a formal program evaluation. The evaluation concluded in the first quarter of FY2014. The experience from and evaluation of the pilot audit program provided the Department with an enhanced understanding of current privacy and security risks to health information. The evaluation noted strengths of the program design and suggestions for establishing a permanent program.

OCR is moving forward with planning for a permanent audit program. We will launch Phase 2 of our audit program in early 2016. This phase will test the efficacy of the combination of desk reviews of policies as well as on-site reviews; it will target specific common areas of noncompliance; and it will include HIPAA business associates. Key activities over the next several months include updating the audit protocols, refining the pool of potential audit subjects, and implementing a screening tool to assess size, entity type, and other information about potential audit subjects. OCR is also updating its electronic document management and investigations tracking system, called the Program Information Management System (PIMS), to build capacity to support an internal audit program. However, while OCR is moving forward with Phase 2, the scope and structure of the audit program long-term will ultimately depend upon the availability and allocation of resources for the program.

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 and the resources required to implement such an enhancement to PIMS.

OIG Recommendation

The OIG recommends that OCR develop an efficient method in PIMS to search for and track covered entities' history of investigations.

OCR Response

OCR concurs with this recommendation. OCR improved its reporting capabilities with respect to open and closed cases in 2014, and it is now possible to track all open and closed investigations in PIMS As such, OCR has the capability to search for and track covered entities' history of compliance.

OIG Recommendation

The OIG recommends that OCR develop a policy requiring OCR staff to check whether covered entities were previously investigated.

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. As noted above, we are now able to check PIMS for covered entities' history of noncompliance; specifically, whether they have been investigated previously. As such, OCR will develop internal guidance, as well as a standardized process, that will require all OCR investigators to check for prior investigations of covered entities or business associates upon the initiation of a new 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 consumer awareness and industry compliance with the HIPAA Rules. 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 sample business associate agreement provisions, guidance on de-identification, fact sheets on numerous Privacy Rule provisions, and, in coordination with the Office of the National Coordinator for Health Information Technology, model notices of privacy practices; and (4) participating in speaking events and webinars on 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 Linda Min 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 Christina Lester. 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.