Department of Health and Human Services
Office of Inspector General
Office of Audit Services

November 2024 | A-18-21-08014

The Office for Civil Rights Should Enhance Its HIPAA Audit Program to Enforce HIPAA Requirements and Improve the Protection of Electronic Protected Health Information

REPORT HIGHLIGHTS

November 2024 | A-18-21-08014

The Office for Civil Rights Should Enhance Its HIPAA Audit Program to Enforce HIPAA Requirements and Improve the Protection of Electronic Protected Health Information

Why OIG Did This Audit

- The increase in the number of successful cyberattacks against health care organizations' information technology (IT) systems raises the question of whether OCR's audits, guidance, and enforcement activities for ensuring the protection of electronic protected health information (ePHI) have been effective. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required HHS to develop national standards for the use and dissemination of health care information, including standards to protect ePHI.
- In this audit, OIG evaluated OCR's program for performing periodic HIPAA audits, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

What OIG Found

OCR fulfilled its requirement under the HITECH Act to perform periodic HIPAA audits. However:

- OCR's HIPAA audit implementation was too narrowly scoped to effectively assess ePHI protections and demonstrate a reduction of risks within the health care sector. Specifically:
    - OCR's audits consisted of assessing only 8 of 180 HIPAA Rules requirements; and
    - only 2 of those 8 requirements were related to Security Rule administrative safeguards and none were related to physical and technical security safeguards.
- OCR oversight of its HIPAA audit program was not effective at improving cybersecurity protections at covered entities and business associates.

What OIG Recommends

We made a series of recommendations to OCR to enhance its HIPAA audit program, including that it expand the scope of its HIPAA audits to assess compliance with physical and technical safeguards from the HIPAA Security Rule, document and implement standards and guidance for ensuring that deficiencies identified during the HIPAA audits are corrected in a timely manner, and define metrics for monitoring the effectiveness of OCR's HIPAA audits at improving audited covered entities and business associates' protections over ePHI and periodically review whether these metrics should be refined. The full recommendations are in the report.

OCR did not concur with one recommendation but concurred with our three other recommendations and detailed steps it has taken and plans to take in response.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

In recent years, cyberattacks, including ransomware attacks, have impacted health care providers' operations and could affect patient care and safety.[1] In its report to Congress for calendar year 2022, the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) stated that it received 64,592 reported breaches affecting 42 million individuals and that the majority of the security incidents associated with these reported breaches were related to the hacking of health care providers.[2] The report also stated that, between 2018 and 2022, the number of reported breaches increased.

In October 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency, the Department of Justice's Federal Bureau of Investigation, and HHS issued a joint cybersecurity advisory stating that threat actors have continued to develop new functionality and tools that increase the ease, speed, and profitability for performing ransomware attacks.[3] The increase in the number of successful cyberattacks against health care entities' information technology (IT) systems raises the question of whether OCR's audits, guidance, and enforcement activities for ensuring the protection of electronic protected health information (ePHI) have been effective. In addition, a 2013 Office of Inspector General (OIG) audit found that OCR had not assessed the risks, established priorities, or implemented controls for the Health Information Technology for Economic and Clinical Health (HITECH) Act requirement that it perform periodic audits of covered entities and business associates (collectively referred to as entities) to ensure their compliance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule requirements.[4] These periodic audits are known as HIPAA audits.

[1] The Journal of the American Medical Association, *Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016–2021*. Accessed on Feb. 6, 2023.

[2] OCR, *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022*. Accessed on Apr. 8, 2024.

[3] *Ransomware Activity Targeting the Healthcare and Public Health Sector*. Accessed on Apr. 22, 2024.

[4] OCR, *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), Nov. 21, 2013.

OBJECTIVES

The objectives of our audit were to determine whether:

- OCR fulfilled the requirement under the HITECH Act to perform periodic audits of entities to assess compliance with HIPAA Privacy, Security, and Breach Notification Rules;

- OCR's HIPAA audit implementation and its audit protocol have been effective in assessing ePHI protections and reducing risks within the health care sector;[5] and

- OCR's oversight of its HIPAA audit program was effective at improving cybersecurity protections at entities.

BACKGROUND

Health Insurance Portability and Accountability Act of 1996

HIPAA required HHS to develop national standards for the use and dissemination of health care information, including standards to protect ePHI. To satisfy the requirement, HHS published the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules). Specifically:

- The Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164) provides Federal protection for the confidentiality of individually identifiable health information created or received by entities.

- The Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) requires reasonable and appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

- The Breach Notification Rule (45 CFR §§ 164.400–414) requires HIPAA covered entities to provide notification following a breach of unsecured protected health information.

HIPAA Rules Implementation and Enforcement Delegated to the Office for Civil Rights

On December 28, 2000, the HHS Secretary published a final rule that delegated to the Director for OCR the authority to implement and enforce the Privacy Rule and impose civil money penalties, under section 1176 of the Social Security Act, for a covered entity's failure to comply with certain requirements and standards (65 Fed. Reg. 82462, 82472 (Dec. 28, 2000)). On August 4, 2009, the HHS Secretary published a notice that delegated to the Director for OCR the

[5] OCR's audit implementation between 2016 and 2020 used selected elements from its comprehensive audit protocol to assess the policies and procedures adopted by entities to meet the HIPAA Rules.

authority to administer, impose civil money penalties, and to make decisions regarding the interpretation and enforcement of the Security Rule (74 Fed. Reg. 38640 (Aug. 4, 2009)).

Health Information Technology for Economic and Clinical Health Act

As part of the American Recovery and Reinvestment Act of 2009 (P.L. No. 111-5), Congress enacted the HITECH Act.[6] The Act promotes the adoption and use of health information technology and notably extends the HIPAA Rules and related criminal and civil penalties to business associates of covered entities, requires HHS to conduct periodic audits of entities to ensure compliance with the HIPAA Rules, and requires HHS to provide an annual report to Congress on HIPAA Rules Compliance (the HITECH Act §§ 13401; 13411; and 13424). The HITECH Act also requires HHS to annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the Security Rule (the HITECH Act § 13401(c)).[7] Congress amended the HITECH Act on January 5, 2021.[8]

HIPAA Enforcement Rule

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings. The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E.

The Office for Civil Rights

OCR's mission is to ensure compliance with our nation's civil rights, conscience and religious freedom, and health information privacy and security laws by investigating complaints and conducting compliance reviews, requiring corrective and remedial action, issuing policy and regulations, and providing technical assistance and public education for the American people.

Through its HIPAA Audit Program, OCR conducts audits of entities to evaluate their adherence to the HIPAA Rules. OCR developed and published what it considered a comprehensive audit protocol that includes the procedures that OCR's auditors use to evaluate an entity's

[6] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act, P. L. No. 111-5 (Feb. 17, 2009), are collectively cited as the HITECH Act.

[7] The HITECH Act mandates HHS to annually provide guidance on effective technical safeguards for implementing the HIPAA Security Rule.

[8] The amendment required HHS to consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place that may mitigate fines, result in early, favorable termination of an audit, or mitigate the remedies agreed to in an agreement resolving potential violations of the HIPAA Security Rule between OCR and the entity.

compliance with the HIPAA Rules.[9] Beginning in 2011, OCR implemented a pilot audit program (Phase 1) to assess the controls and processes implemented by 115 covered entities to comply with HIPAA's requirements. Between 2016 and 2017 (Phase 2), OCR audited entities' compliance with the HIPAA Rules by assessing 207 entities against selected elements from its comprehensive audit protocol.[10] OCR used contractors to assist with these audits. If an audit report indicates a serious compliance issue, OCR may initiate a compliance review to further investigate. See Appendix B for additional information on OCR's HIPAA Rules enforcement process.

Prior Office of Inspector General Audit Results

In our 2013 audit, we found that OCR met some Federal requirements related to overseeing and enforcing the Security Rule.[11] Specifically, OCR provided guidance to entities that promoted compliance with the Security Rule and established an investigation process for responding to reported Security Rule violations. OCR also followed Federal regulations when imposing penalties for Security Rule violators. However, OCR did not meet other Federal requirements critical to the oversight and enforcement of the Security Rule. OIG found the following:

> Although OCR made available to covered entities guidance that promoted compliance with the Security Rule, it had not assessed the risks, established priorities, or implemented controls for its HITECH requirement to provide for periodic audits of covered entities to ensure their compliance with Security Rule requirements. As a result, OCR had limited assurance that covered entities complied with the Security Rule and missed opportunities to encourage those entities to strengthen their security over ePHI.

OIG made multiple recommendations to OCR, including that it perform periodic audits in accordance with the HITECH Act to ensure entities complied with the Security Rule.

Current Health Care Sector Threat Landscape

OCR recognizes that threats against the health care sector remain high. Between 2016 and 2022, reported breaches affecting fewer than 500 individuals increased 10 percent and the

[9] Available online at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html. OCR developed the protocol that they use as part of its audit program and posted it online for entities to use when evaluating their compliance with these rules.

[10] We use the word "elements" because OCR organized its audit protocol by numbered elements that contain audit analysis requirements for one or more standards of the Rules.

[11] See footnote 4.

number of breaches affecting 500 or more individuals increased by 87 percent.[12] (See Figures 1 and 2 below.)

Figure 1: Reported Breaches Affecting Under 500 Individuals

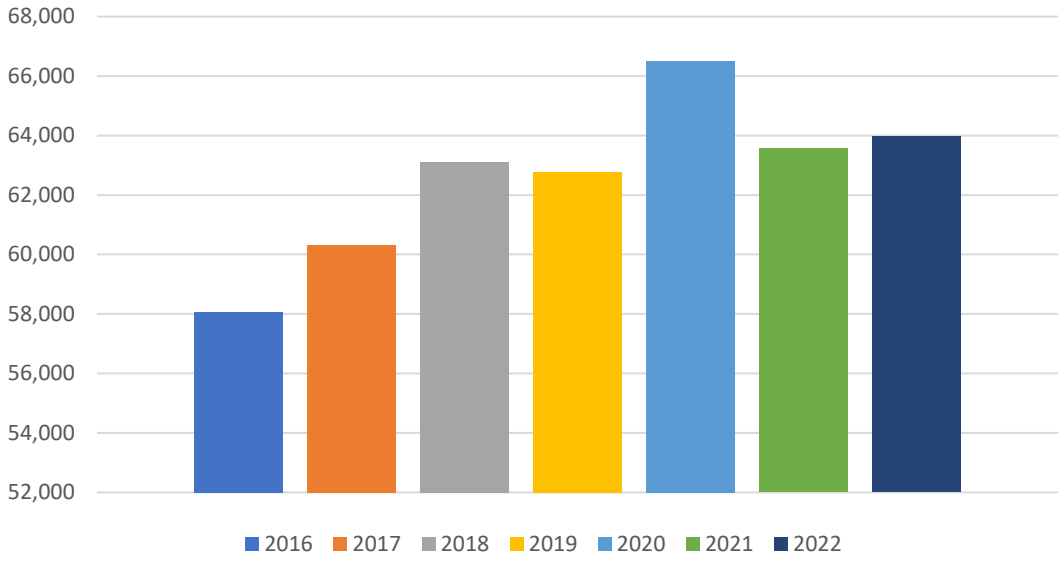
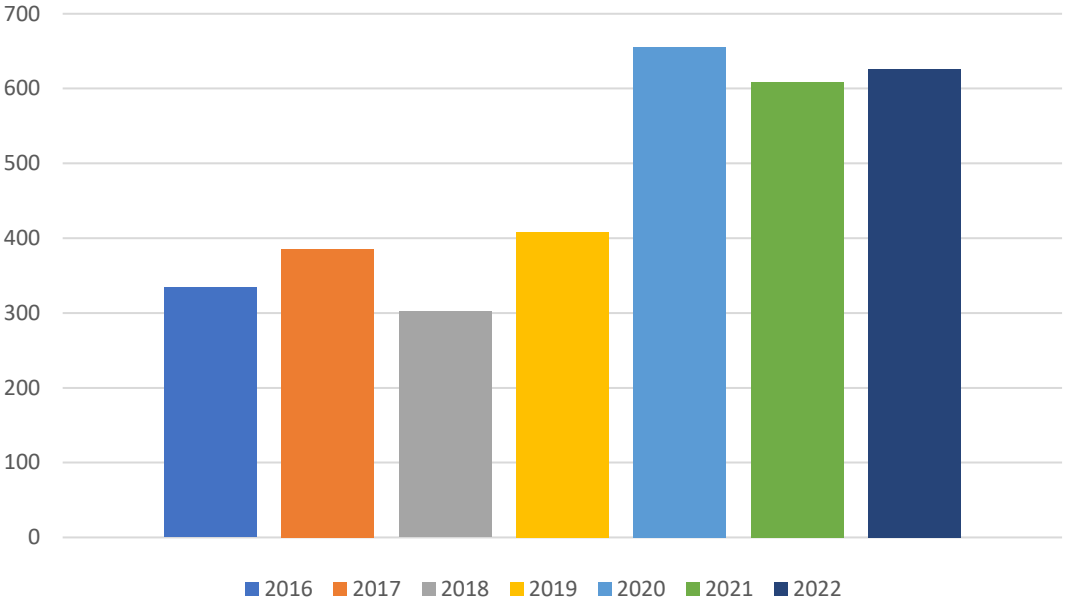


Figure 2: Reported Breaches Affecting Over 500 Individuals



[12] Data from OCR's annual reports to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for calendar years 2020 through 2022.

In an October 31, 2023, email to recipients of an OCR online mailing list, OCR stated that:

> [r]ansomware and hacking are the primary cyber-threats in health care. In the past four years, there has been a 239% increase in large breaches reported to OCR involving hacking and a 278% increase in ransomware. This trend continues in 2023, where hacking accounts for 77% of the large breaches reported to OCR. Additionally, the large breaches reported this year [2023] have affected over 88 million individuals, a 60% increase from last year.

The American public has witnessed disruptive attacks on its health care sector that jeopardize sensitive personal information, delay medical treatment, and ultimately may lead to increased suffering and death. Recently, the *Journal of the American Medical Association* issued the result of its group study on 374 ransomware attacks against health care delivery organizations that found that "ransomware attacks exposed larger quantities of personal health information and grew more likely to affect large organizations with multiple facilities."[13]

HOW WE CONDUCTED THIS AUDIT

We audited how OCR administered its HIPAA audit program from January 2016 through December 2020, which included a review of 30 of the 207 final HIPAA audit reports and related documents that were produced by OCR during that timeframe.[14, 15] We reviewed the statutory requirements in HITECH, the regulatory requirements of the HIPAA Enforcement Rule, and OCR's policies and procedures for implementing HITECH requirements and enforcing HIPAA Rules. We also reviewed OCR reports to Congress on HIPAA Rules Compliance, as well as cyber-related guidance OCR provided to the health care industry from 2016 to 2020. In addition, we reviewed OCR's HIPAA audit protocol and selected OCR policies and procedures.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A contains the details of our audit scope and methodology and Appendix C contains the Federal requirements we used to evaluate OCR's controls.

[13] "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," *Journal of the American Medical Association*, Dec 29, 2022.

[14] During our audit period, OCR only performed audits between 2016 and 2017.

[15] The 30 audits were of hospitals and health systems.

FINDINGS

OCR fulfilled its requirement under the HITECH Act to perform periodic audits of entities' compliance with the HIPAA Rules. Although OCR implemented its audit program to periodically assess the ePHI protections using the audit protocols it developed, OCR's HIPAA audit implementation did not include assessing the majority of the required protections for compliance with the HIPAA Rules. In 2016 and 2017, OCR's HIPAA Audit Program consisted of performing desk audits of selected entities and did not include assessing most of the requirements contained in its comprehensive audit protocol. The audits consisted of assessing only 8 of 180 HIPAA Rules requirements included in OCR's audit protocol. Of those eight, OCR's audits included only two Security Rule administrative safeguards and no physical and technical security safeguards. OCR chose the two safeguards because audits that it conducted in 2012 identified that entities struggled to implement the Security Rule's requirements for security risk analysis and risk management, consistent with OCR's findings in investigations and enforcement actions. However, assessing two administrative security requirements is generally not sufficient to assess the risk within the healthcare sector and to determine the effectiveness of the ePHI security protections that should be in place, as required by the Security Rule. In addition, because of their narrow scope, the HIPAA audits most likely did not identify entities, such as hospitals that did not implement the physical and technical safeguards defined in the Security Rule to protect ePHI against common cybersecurity threats.

OCR oversight of its HIPAA audits program likely was not effective at improving cybersecurity protections at entities. Further, its HIPAA audits did not include certain elements to address and monitor HIPAA Rules compliance. For example, OCR did not require audited entities to respond to deficiencies by implementing corrective actions and confirming implementation. In addition, OCR did not monitor HIPAA audit program outcomes. This occurred because OCR lacked a documented process and procedures for conducting these audit steps, including for timely resolving identified deficiencies. Without responses from entities, OCR does not have commitments that corrective actions have been or will be implemented to address deficiencies which, if left unaddressed, could impact patient data, care, and safety.

Also, OCR did not define when it would initiate compliance reviews if serious compliance issues were identified during HIPAA audits. Although OCR indicated that it may initiate a separate compliance review for serious compliance issues identified during HIPAA audits, it rarely initiated these reviews when it identified serious compliance issues. OCR oversight of its HIPAA audit program could have been more effective at improving cybersecurity protections at entities if it initiated separate compliance reviews as part of its audit program. Additionally, as of 2020, OCR had not documented the frequency of its HIPAA audits. Further, OCR has not conducted any HIPAA audits since 2017 and missed the opportunity during this period to proactively identify audited entities' noncompliance with the HIPAA Rules. Without defined HIPAA audit program policies, processes, outcomes, and monitoring, OCR is unlikely to be able to determine whether its current audit program efforts are effective in helping protect ePHI and improving cybersecurity protections at entities.

THE OFFICE FOR CIVIL RIGHTS MET THE HITECH ACT AUDIT REQUIREMENT

The HITECH Act stipulates that HHS must provide for periodic audits (HIPAA audits) to ensure that entities subject to the requirements of the HIPAA Rules comply with such requirements. OCR fulfilled its requirement under the HITECH Act to perform periodic audits of entities. Specifically, OCR performed 207 audits (166 covered entities and 41 business associates) between 2016 and 2020. In many cases, OCR's audit results demonstrated that the audited entities made negligible efforts to comply or did not provide evidence of a serious attempt to comply with the HIPAA Rules.

THE OFFICE FOR CIVIL RIGHTS' HIPAA AUDITS DID NOT FULLY ASSESS ELECTRONIC PROTECTED HEALTH INFORMATION REQUIREMENTS

The HITECH Act mandates that HHS shall provide for periodic audits to ensure that entities that are subject to HIPAA Rules requirements comply with such requirements.

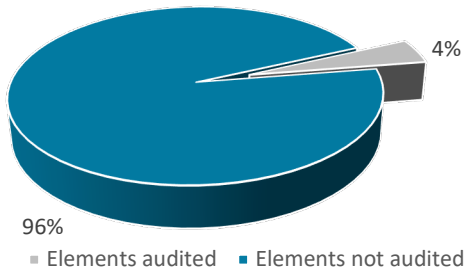
During Phase 2 of HIPAA audit program, OCR focused on testing the utility and cost effectiveness of its desk audits of entities.[16] OCR originally planned to include in its audit program (1) over 200 desk audits that would evaluate entities' compliance with selected HIPAA Rules requirements and (2) a smaller number of comprehensive on-site audits that would evaluate entities against a comprehensive set of HIPAA compliance provisions. OCR intended to use its HIPAA audits to identify promising practices for protecting the privacy and security of health information and discover risks and vulnerabilities that may not have been revealed by OCR's enforcement activities. As of June 2024, OCR had completed only the desk audits and, in its report to Congress for calendar year 2022 (issued in 2024), OCR reported that it has not initiated any additional audits due to a lack of financial resources.[17]

[16] In 2011 and 2012, OCR implemented a pilot audit program (Phase 1) to assess the controls and processes implemented by 115 covered entities to comply with HIPAA's requirements. OCR's 2016 HIPAA Audit Program (Phase 2) reviewed the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.

[17] *Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2022* (issued Feb. 22, 2024). Accessed on May 28, 2024.

OCR also developed what it deemed a comprehensive audit protocol for use in the audits to analyze an entity's compliance with the HIPAA Rules. However, Phase 2 of OCR's HIPAA audit program did not include fully assessing compliance with the required ePHI protections. The audits assessed compliance with 8 or fewer of the 180 elements in its published audit protocol (Figure 3 shows the percentage of elements in the published HIPAA audit protocol covered by OCR's desk audits). These eight elements only included assessing two Security Rule administrative safeguards (Risk Analysis and Risk Management), three Privacy Rule provisions (Notice of Privacy Practices and Content Requirements, Provision of Notice, and Right of Access), and three Breach Notification Rule provisions (Timeliness of Notification, Content of Notification, and Notification by a Business Associate (assessed only at Business Associates)).[18, 19] The audits were narrowly scoped to certain issues identified during the audits OCR conducted between 2011 and 2012. The audits did not include assessing requirements such as the Security Rule physical and technical safeguards, which protect entities and their systems from unauthorized intrusion and access to ePHI. Therefore, OCR missed the opportunity to identify physical and technical deficiencies that should be remediated to reduce risks within the health care sector. Further, entities' ePHI may be vulnerable to compromise by bad actors or accidental exposure by an unintentional mishap.

Figure 3



THE OFFICE FOR CIVIL RIGHTS' OVERSIGHT OF ITS HIPAA AUDITS PROGRAM WAS NOT EFFECTIVE AT IMPROVING CYBERSECURITY PROTECTIONS AT ENTITIES

Office of Management and Budget (OMB) Circular No. A-123 mandates agencies to integrate risk management and internal control functions, aligning with the Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* (Green Book). It emphasizes establishing and monitoring performance measures for management objectives to ensure expected outcomes in major Federal Government programs. Within HHS, OCR has responsibility for enforcing the HIPAA Rules and will attempt to resolve compliance issues by obtaining voluntary compliance, implementing corrective action, establishing resolution agreements, or imposing civil money penalties for an entity's failure to comply with certain

[18] The Security Rule defines administrative safeguards in § 164.304 as "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." Available online at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf. Accessed on Dec. 1, 2023.

[19] None of the 207 audits included all 8 elements.

requirements and standards. OCR is also required to annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the Security Rule.

OCR offered guidance to entities to promote compliance with the Security Rule. However, OCR did not require audited entities to remedy deficiencies by implementing corrective actions and confirm implementation. Also, OCR did not monitor HIPAA audit program outcomes. OCR oversight of its HIPAA audit program could have been more effective at improving cybersecurity protections at entities if these additional tasks were part of its audit program.

Additionally, OCR did not define when it would initiate compliance reviews when serious compliance issues were found during its HIPAA audits. Although OCR indicated that it may initiate a separate compliance review for serious compliance issues identified during its HIPAA audits, it rarely initiated a compliance review when it identified a serious compliance issue. For example, OCR started 1 compliance review related to the Security Rule and 2 compliance reviews related to Privacy and Breach Notification Rules out of the more than 70 entities that it identified as having serious compliance issues during Phase 2 of its HIPAA audit program.

Further, OCR did not document the frequency of its HIPAA audits as of 2020. OCR has not conducted any HIPAA audits since 2017 and missed the opportunity during this period to proactively identify audited entities' noncompliance with the HIPAA Rules.

OCR did not implement a documented process that laid out the procedures to follow during and after its Phase 2 HIPAA audits to resolve any identified deficiencies. In addition, OCR did not establish a policy to define when compliance reviews should be required as the result of these HIPAA audits.

OCR's lack of documented procedures for responding to deficiencies and serious compliance issues identified in its HIPAA audits, impeded it from determining whether its HIPAA audit program efforts were effective in safeguarding ePHI and improving cybersecurity protections at entities. Without responses from entities regarding the deficiencies identified in OCR's HIPAA audits, OCR did not have the commitment from audited entities that corrective actions have been or will be implemented. If deficiencies were left unaddressed, they could negatively impact patient data, care, and safety. In addition, OCR oversight of its HIPAA audits may have missed an opportunity to help improve cyber protections at audited entities by requiring deficiencies be corrected. Further, without defined HIPAA audit program policies, processes, outcomes, and monitoring, OCR is unlikely to be able to determine whether its current audit program efforts are effective in helping protect ePHI and improving cybersecurity protections at entities.

RECOMMENDATIONS

We recommend that the Office for Civil Rights:

- expand the scope of its HIPAA audits to assess compliance with physical and technical safeguards from the Security Rule;

- document and implement standards and guidance for ensuring that deficiencies identified during the HIPAA audits are corrected in a timely manner;

- define and document criteria for determining whether a compliance issue identified during a HIPAA audit should result in OCR initiating a compliance review; and

- define metrics for monitoring the effectiveness of OCR's HIPAA audits at improving audited entities' protections over ePHI and periodically review whether these metrics should be refined.

OFFICE FOR CIVIL RIGHTS COMMENTS

In written comments on our draft report, OCR concurred with three of our four recommendations and described actions it has taken or plans to take to address them.

OCR concurred with our first recommendation, contingent upon it receiving appropriate funding. Further, OCR indicated that, due to limited financial and staffing resources, it cannot audit every provision within the HIPAA Rules. OCR stated that it will focus future audits on specific provisions based on a variety of factors, including industry trends and prevalent risks to protected health information. OCR indicated that future audits may include selected provisions from the HIPAA Security Rule, including physical or technical safeguards.

OCR did not concur with our second recommendation. Specifically, OCR stated that, under the HITECH Act, entities can choose to pay civil money penalties instead of addressing HIPAA deficiencies through corrective action plans and cannot be compelled to sign resolution agreements or promptly correct issues. OCR indicated that it has requested legislation from Congress to authorize it to seek injunctive relief, which would enable OCR to collaborate with the Department of Justice to pursue remedies in Federal court to secure compliance with the HIPAA Rules.[20] Further, OCR stated that it does not have the financial or staff resources to pursue corrective action plans or penalties for every entity with HIPAA deficiencies and stated that the process of negotiating resolution and initiating formal enforcement actions is resource-intensive and would hinder other essential investigations. OCR also stated that HIPAA audits were designed to be voluntary and intended to provide technical assistance rather than enforce

[20] Injunctive relief is a legal remedy in the form of a court order that requires a party to do (or to refrain from doing) certain acts. It is a preventative measure aimed at stopping potential or ongoing harm that cannot be adequately compensated by damages.

corrections. OCR stated that imposing requirements for audited entities to correct deficiencies in a timely manner could discourage entities from participating in HIPAA audits. Finally, OCR stated that it agrees with implementing criteria for follow-up compliance reviews; however, it noted that entities would still have the option to pay a civil money penalty rather than correcting deficiencies.

OCR concurred with our third recommendation and stated that it plans to initiate additional HIPAA audits later this year. OCR stated that it will also establish criteria to determine whether to initiate follow-up compliance reviews for entities that have been audited and found to have HIPAA compliance issues if these issues are not corrected during the audit.

OCR concurred with our fourth recommendation and stated that, after receiving a similar recommendation from the Government Accountability Office, it created a survey to be sent to entities that have participated in HIPAA audits. OCR stated that it plans to use the results of the survey in future HIPAA audits and as a mechanism to track how audited entities made changes to their compliance with HIPAA following an audit.

OCR's comments are included in their entirety as Appendix D.

OFFICE OF INSPECTOR GENERAL RESPONSE

OIG acknowledges that OCR faces significant challenges in managing the HIPAA Rules, which may limit its ability to implement additional compliance tools. We encourage OCR to continue to request the necessary funding, personnel, and other resources it needs to conduct its HIPAA audits and enforce the HIPAA Rules, especially as the number of cybersecurity and privacy threats continue to increase. We remain concerned that OCR's HIPAA audits, as implemented, do not provide assurance that audited entities are complying with the HIPAA Rules requirements.

Regarding OCR's response to our second recommendation, we acknowledge that OCR chose to make participation in HIPAA audits voluntary; however, we disagree with OCR's interpretation of the potential effect of civil money penalties. The primary goal of these audits is for OCR to ensure that entities comply with HIPAA regulations to protect the privacy and security of protected health information (PHI). Furthermore, although the HITECH Act does not specify that entities must resolve HIPAA audit deficiencies, OCR's response omitted that entities still have to comply with the HIPAA Rules and that civil money penalties payments do not relieve entities from compliance. Even after a civil money penalty is imposed, the entity would need to take necessary steps to correct the unresolved, identified deficiencies to be in compliance with the HIPAA Rules. Therefore, entities must address any significant deficiencies OCR identified in the audits. We maintain the validity of our recommendation to OCR to document and implement standards and guidance for ensuring that deficiencies identified during HIPAA audits are corrected in a timely manner to protect PHI. We are encouraged by OCR's efforts to seek authority for injunctive relief and believe that a requirement for entities to promptly correct any identified deficiencies should be included in such relief. In the interim, OCR should inform

all future audited entities that failure to correct identified deficiencies during these audits may lead to compliance reviews and potential civil money penalties.

Although we have not yet confirmed whether OCR effectively implemented our recommendations, we are encouraged by OCR's comments. We look forward to receiving and reviewing documentation related to OCR's implementation through our audit resolution process.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We assessed the implementation of OCR's HIPAA audit program during the audit period January 2016 through December 2020 and examined 30 final HIPAA audit reports and related documentation. We also assessed OCR reports to Congress and the health care industry. In addition, we assessed OCR's HIPAA audit protocol, OCR's HIPAA audit program oversight, and OCR policies and procedures for enforcing the HIPAA Rules.

We reviewed OCR's statutory requirements under HIPAA and the HITECH Act, the regulatory requirements in the HIPAA Enforcement Rule, policies and procedures enforcing the HIPAA Rules and HITECH requirements, the HIPAA audit program and audit protocol, and cyber-related guidance issued to entities.

We did not assess OCR's overall internal controls. Rather, we limited our review of internal controls to those applicable to our audit objective. This included assessing whether OCR: 1) established program outcomes and metrics and monitored whether they were being met and 2) monitored the status of remediation efforts through completion. We also assessed the policies, procedures, and practices applicable to the HITECH Act requirement for OCR to perform audits to ensure compliance with the HIPAA Rules.

We conducted audit work remotely from April 2021 through June 2024.

METHODOLOGY

To accomplish our objectives, we:

- reviewed applicable Federal laws, regulations, and guidance;
- analyzed data from OCR's list of reported breaches of unsecured protected health information;[21]
- reviewed OCR's reports to Congress and its *2016-2017 HIPAA Audits Industry Report* to gather details regarding the audits performed by OCR;
- interviewed OCR management to gain an understanding of OCR's HIPAA audit and enforcement process;
- evaluated OCR's HIPAA and HITECH enforcement process for entities by interviewing OCR officials and reviewing enforcement documentation provided by OCR officials;

[21] As required by the HITECH Act § 13402(e)(4), the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals.

- assessed the implementation of OCR's audit program and audit protocol by reviewing 30 final HIPAA audit reports and related documentation;

- reviewed OCR's HIPAA audit standard operating procedures;

- reviewed contracts between OCR and vendors for audit services used during the 2016-2017 audits to determine performance metrics;

- reviewed OCR public communications to determine what cybersecurity guidance OCR issued to industry stakeholders;

- reviewed draft and final audit reports, including entities' responses to the reports, for the 30 of the 207 hospitals and health systems selected by OCR for a HIPAA audit between 2016 and 2020, to assess whether entities effectively addressed OCR audit findings; and

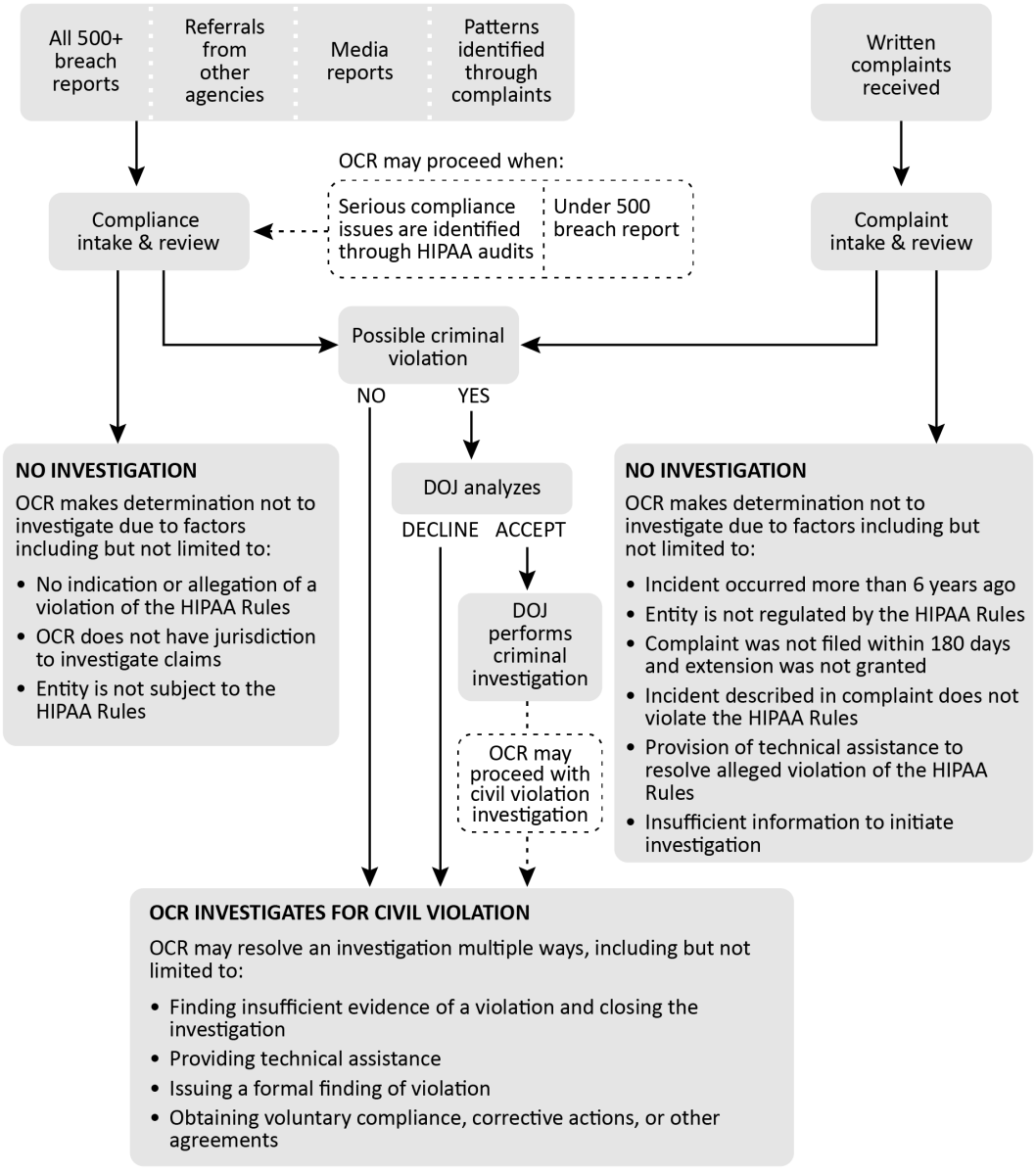
- discussed the results of our audit with OCR officials.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: THE OFFICE FOR CIVIL RIGHTS' PROCESS FOR ENFORCING THE HIPAA RULES

OCR begins its HIPAA Rules enforcement process by reviewing written complaints received, either on paper, by e-mail, through its complaint portal, through an event or incident brought to OCR's attention (e.g., breach reports, media, referrals from other agencies), or patterns identified through the complaints received. If OCR identifies a serious compliance issue during its HIPAA audits, OCR may initiate a compliance review. See Figure 4 below for a description of OCR's enforcement process.

Figure 4: OCR HIPAA Rules Enforcement Process



As part of its enforcement process, OCR may conduct compliance reviews to determine whether entities comply with the HIPAA Rules. Further, OCR's enforcement process includes

conducting audits and providing education and outreach to support compliance with the HIPAA Rules. When necessary, OCR has the authority to issue subpoenas to compel cooperation with an investigation. Following is a description of the actions OCR takes as part of its enforcement process:

COMPLIANCE REVIEWS

One method that OCR uses to determine compliance with the HIPAA Rules is through compliance reviews. OCR opens compliance reviews for all reports of breaches affecting 500 or more individuals and for some reports of breaches affecting fewer than 500 individuals. OCR may also open a compliance review of an entity based on an event or incident brought to OCR's attention through the media, a referral from another agency, or patterns identified through complaints.

INVESTIGATIONS

Once OCR starts an investigation, either from a complaint or a compliance review, OCR collects evidence through interviews, witness statements, requests for data from the entity involved, site visits, or other available relevant documents. Entities are required by law to cooperate with complaint investigations and compliance reviews.

OCR may determine, based on the evidence, that the entity was not in compliance with the HIPAA Rules. In such cases, OCR will generally first attempt to resolve the case by providing entities the opportunity to voluntarily comply and address the potential violation(s) through corrective actions that OCR defines, which may include a resolution agreement.

Where corrective action is sought, OCR obtains satisfactory documentation and other evidence from the entity that it undertook the required corrective action to resolve the potential HIPAA violations. In most cases, an entity will, through voluntary cooperation and corrective action, be able to show satisfactory compliance with the HIPAA Rules.

AUDITS

Section 13411 of the HITECH Act requires HHS to perform periodic audits (known as HIPAA audits) of covered entities and business associates to ensure compliance with the HIPAA Rules. For the HIPAA audits performed between 2016 and 2017, OCR's audit objectives were to: (1) assess entities' efforts to comply with the HIPAA Rules, (2) ensure that entities were adequately safeguarding PHI, and (3) ensure that individuals were provided the rights afforded to them by the HIPAA Rules.

RESOLUTION AGREEMENTS

Where OCR finds indications of noncompliance due to willful neglect, or where the nature and scope of the noncompliance warrants additional enforcement action, OCR pursues a resolution

agreement with a payment of a settlement amount and an obligation to complete a corrective action plan. Additionally, in most cases, the resolution agreement requires the covered entity or business associate to fix remaining compliance issues and to undergo OCR monitoring of its compliance with the HIPAA Rules for a specified time.

CIVIL MONEY PENALTIES

If OCR and a covered entity or business associate are unable to reach a satisfactory agreement to resolve the matter informally, or if a covered entity or business associate breaches the terms of a resolution agreement, OCR may pursue formal enforcement. In such cases, OCR notifies the covered entity or business associate of a proposed determination of a violation of the HIPAA Rules and OCR's intent to impose a civil money penalty.

APPENDIX C: FEDERAL REQUIREMENTS

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT REQUIREMENTS

HITECH Act § 13401 (c) Annual Guidance

> For the first year beginning after the date of the enactment of this Act and annually thereafter, the Secretary of Health and Human Services shall, after consultation with stakeholders, annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations, including the use of standards developed under section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by section 13101 of this Act, as such provisions are in effect as of the date before the enactment of this Act.

HITECH Act § 13411 Audits

> The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act, comply with such requirements.

HITECH Act § 13424(1) Studies, Reports, Guidance

> For the first year beginning after the date of the enactment of this Act and annually thereafter, the Secretary shall prepare and submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Ways and Means and the Committee on Energy and Commerce of the House of Representatives a report concerning complaints of alleged violations of law, including the provisions of this subtitle as well as the provisions of subparts C and E of part 164 of title 45, Code of Federal Regulations, (as such provisions are in effect as of the date of enactment of this Act) relating to privacy and security of health information that are received by the Secretary during the year for which the report is being prepared.

FEDERAL REGULATIONS: SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

Federal regulations (45 CFR § 164.306 (c)) state that "a covered entity or business associate must comply with the applicable standards as provided in this section and in

§§ 164.308, 164.310, 164.312, 164.314 and 164.316 with respect to all electronic protected health information."

SECRETARIAL ACTION REGARDING COMPLAINTS AND COMPLIANCE REVIEWS

Federal regulations (45 CFR § 160.312), *Secretarial action regarding complaints and compliance reviews* state:

(a) Resolution when noncompliance is indicated.

(1) If an investigation of a complaint pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.

(2) If the matter is resolved by informal means, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

(3) If the matter is not resolved by informal means, the Secretary will—

(i) So inform the covered entity or business associate and provide the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under §§ 160.408 and 160.410 of this part. The covered entity or business associate must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of such notification; and

(ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity or business associate of such finding in a notice of proposed determination in accordance with § 160.420 of this part.

(b) Resolution when no violation is found. If, after an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

BASIS FOR A CIVIL MONEY PENALTY

Federal regulations (45 CFR § 160.402 (a)) state that "the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision."

FEDERAL INTERNAL CONTROL REQUIREMENTS

OMB Circular No. A-123 requires agencies to integrate risk management and internal control functions. The Circular also establishes an assessment process based on Green Book.

In addition, OMB A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," states that "[m]anagement is also responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance. Management must consistently apply these internal control standards to meet the internal control principles and related components outlined in this circular and to assess and report on internal control effectiveness at least annually."

GAO's Green Book requires agencies to adhere to principles, including:

Principle 6 – Define Objectives and Risk Tolerances

> 6.04: Management defines objectives in measurable terms so that performance toward achieving those objectives can be assessed. Measurable objectives are generally free of bias and do not require subjective judgments to dominate their measurement. Measurable objectives are also stated in a quantitative or qualitative form that permits reasonably consistent measurement.
>
> 6.07: Management determines whether performance measures for the defined objectives are appropriate for evaluating the entity's performance in achieving those objectives. For quantitative objectives, performance measures may be a targeted percentage or numerical value. For qualitative objectives, management may need to design performance measures that indicate a level or degree of performance, such as milestones.

Principle 10 - Design Control Activities

> 10.03: Management designs appropriate types of control activities for the entity's internal control system. Control activities help management fulfill responsibilities and address identified risk responses in the internal control system. The common control activity categories listed in figure 6 are meant only to illustrate the range and variety of control activities that may be useful to management. The list is not all inclusive and may not include particular control activities that an entity may need.

Establishment and review of performance measures and indicators

Management establishes activities to monitor performance measures and indicators. These may include comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken. Management designs controls aimed at validating the propriety and integrity of both entity and individual performance measures and indicators.

Principle 17 – Evaluate Issues and Remediate Deficiencies

Corrective Actions

17.06: Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis. These corrective actions include resolution of audit findings. Depending on the nature of the deficiency, either the oversight body or management oversees the prompt remediation of deficiencies by communicating the corrective actions to the appropriate level of the organizational structure and delegating authority for completing corrective actions to appropriate personnel. The audit resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates that the findings and recommendations do not warrant management action. Management, with oversight from the oversight body, monitors the status of remediation efforts so that they are completed on a timely basis.

APPENDIX D: OFFICE FOR CIVIL RIGHTS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

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

DATE: August 14, 2024

TO: Amy J. Frontz
Deputy Inspector General for Audit Services

FROM: Melanie Fontes Rainer
Director
Office for Civil Rights

SUBJECT: Office of Inspector General (OIG) Draft Report: "The Office for Civil Rights Should Enhance Its HIPAA Audit Program to Enforce HIPAA Requirements and Improve the Protection of Electronic Protected Health Information," A-18-21-08014

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 whether: (1) OCR fulfilled the requirement under the HITECH Act to perform periodic audits of covered entities and business associates to assess compliance with the HIPAA Privacy, Security, and Breach Notification Rules; (2) OCR's HIPAA audit implementation and its audit protocol have been effective in assessing electronic protected health information (ePHI) protections and reducing risks within the health care sector; and (3) OCR's oversight of its HIPAA audit program was effective in improving cybersecurity protections at covered entities and business associates.

As the office responsible for the administration and enforcement of the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), OCR is committed to compliance with the HIPAA Rules through rulemaking and guidance, compliance and enforcement, and outreach and education. The HITECH Act of 2009 created a requirement for OCR to conduct periodic audits of HIPAA covered entities and business associates to ensure their compliance with the HIPAA Rules. The HIPAA audit program is an integral component of OCR's efforts to improve the privacy and security of individuals' health information.

OCR implemented its audit program by initiating audits in 2012 of 115 covered entities, and in 2016 and 2017 of 166 covered entities and 41 business associates. In 2020, OCR published an industry report sharing the results of the 2016-2017 audits with the regulated industry and the public. OCR's audits have been limited in the number of entities audited, the number of HIPAA provisions that are audited, and the frequency of the audits due to inadequate funding.

As you are aware and has been reported in OCR's Budget request since 2009, OCR has operated on a small budget, even though OCR has submitted significant requests for additional resources

to implement and enforce the HIPAA Rules, including audits.[1] The lack of receipt of these requested additional resources has resulted in less staff and investigators to conduct HIPAA audits more frequently, larger scale, or in greater number due to a lack of sufficient funding to conduct all needed operational activities. Further, there has been a tremendous surge in the volume of complaints (civil rights and HIPAA) and HIPAA large breach reports (affecting 500 or more individuals) that OCR receives annually. From fiscal years 2010 to 2023, OCR's receipt of complaints increased 306% (11,426 to 46,401) and large breach report receipts increased 35,950% (2 to 721). During this same time period, investigative staff decreased 30% (130 to 91), reaching an all-time low in FY 2022 of 60 investigators and an all-time high of 51,779 complaints. Currently, OCR has less than 100 investigators, or less than 2 per each state, which has resulted in unsustainably high caseloads and frequent attrition.

OCR has requested additional appropriations, but such efforts have been unavailing. These financial and staffing limitations have affected OCR's past implementations of its audit program, and until OCR receives additional appropriations, it will continue to effect OCR's future audit activities, and OCR's ability to fully implement all of OIG's recommendations.

OCR appreciates OIG's review and recommendations set forth in its draft report. OCR plans to initiate more HIPAA audits this year with a smaller-scale audit program with its current resources and is seeking information and opportunities to improve our use of, administration of, and education of, audits as a tool to improve HIPAA compliance. OCR's specific response to each of the OIG recommendations follows.

OIG Recommendation

The OIG recommends that OCR expand the scope of its HIPAA audits to assess compliance with physical and technical safeguards from the Security Rule.

OCR Response

OCR concurs with this recommendation with appropriate funding. OCR does not have the financial or staff resources to expand the scope of HIPAA audits to conduct audits of every provision contained within the HIPAA Privacy, Security, and Breach Notification Rules.[2] Given OCR's limited financial and staff resources, in future audits, OCR will continue to select provisions of the HIPAA Rules to assess covered entities' and business associates' compliance. This selection will be based on a variety of factors including current trends within the regulated industry and what are the most prevalent risks and vulnerabilities to protected health information. OCR concurs that future HIPAA audits may include selected provisions from the HIPAA Security Rule, including certain physical or technical safeguard provisions.

---

[1] For example, see HHS FY 2024 and 2025 Budget In Brief; https://www.hhs.gov/about/budget/fy2024/index.html; https://www.hhs.gov/about/budget/fy2025/index.html.

[2] The HIPAA Privacy, Security and Breach Notification Rules' Audit Protocol contain 180 standards and implementation specifications. *See* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html.

OIG Recommendation

The OIG recommends that OCR document and implement standards and guidance for ensuring that deficiencies identified during the HIPAA audits are corrected in a timely manner.

OCR Response

OCR does not concur with this recommendation. First, the HITECH Act gives covered entities and business associates the option to pay a civil money penalty in lieu of resolving an OCR HIPAA investigation with a corrective action plan.[3] The payment of a civil money penalty does not require that the entity paying the civil money penalty also correct HIPAA deficiencies identified by OCR. Similarly, audited entities also cannot be compelled to sign a resolution agreement and agree to a corrective action plan to address identified HIPAA deficiencies in a timely manner. Additionally, OCR has requested legislation from Congress authorizing OCR to seek injunctive relief. With this authority, OCR could work with the U.S. Department of Justice to pursue remedies in federal court to secure compliance with the HIPAA Rules. For example, OCR could seek injunctive relief to compel a covered entity to provide breach notification to affected individuals or to compel an entity to immediately remove individuals' protected health information posted publicly on the internet without authorization. However, without this ability to seek injunctive relief, OCR cannot ensure that deficiencies identified in a HIPAA audit are corrected in a timely manner.

Second, OCR does not have the financial or staff resources to pursue corrective action plans or potential civil money penalties against every audited entity where OCR finds HIPAA deficiencies. Negotiating resolution agreements and corrective action plans or initiating the formal HIPAA enforcement process, which can include the filing of litigation pleadings before an administrative law judge and a potential appeal process are time-consuming and resource-intensive activities, which would impede OCR's ability to complete complaint and breach investigations.

Third, participation in the HIPAA audits was designed to be voluntary for selected HIPAA covered entities and business associates. The goal of the HIPAA audits is for OCR to review willing participants' compliance with selected provisions of the HIPAA Rules, and to provide technical assistance where deficiencies were found. The purpose is to provide technical assistance as an additional HIPAA compliance tool, separate from OCR's regular HIPAA investigation and enforcement activities, which, where potential HIPAA violations are found, can result in a resolution agreement where the covered entity or business associate agrees to implement a corrective action plan to address the identified potential violations, or alternatively, pay a civil money penalty. Adding a requirement for audited entities to correct HIPAA deficiencies in a timely manner may result in fewer covered entities and business associates agreeing to participate in a HIPAA audit, because their participation could result in a resolution agreement and corrective action plan or potential civil money penalty, for identified deficiencies that are not corrected in a timely manner.

[3] A corrective action plan is part of a settlement agreement between OCR and a covered entity or business associate, where they agree to implement certain corrective actions within agreed upon timeframes.

OCR agrees with the OIG recommendation below about implementing criteria for determining whether a compliance issue identified in a HIPAA audit should result in OCR initiating a subsequent compliance review of that audited entity and believes that is the best option for addressing this recommendation. However, in such instances where a compliance review was initiated and potential violations were found, the entity under investigation would still have the option of paying a civil money penalty instead of timely correcting potential HIPAA violations.

OIG Recommendation

The OIG recommends that OCR define and document criteria for determining whether a compliance issue identified during a HIPAA audit should result in OCR initiating a compliance review.

OCR Response

OCR concurs with this recommendation. OCR is planning to initiate HIPAA audits later this year and will develop criteria identifying what factors OCR will consider when deciding whether to initiate a subsequent compliance review of an audited entity where the audit found HIPAA compliance issues and the audited entity has not corrected the issues identified during the audit.

OIG Recommendation

The OIG recommends that OCR define metrics for monitoring the effectiveness of OCR's HIPAA audits at improving audited entities' protections over ePHI and periodically review whether these metrics should be refined.

OCR Response

OCR concurs with this recommendation. OCR received a similar recommendation from the Government Accountability Office and created a survey to be sent to covered entities and business associates that participated in the last HIPAA audit. This survey will be sent later this year, and OCR will use the survey results in future HIPAA audits and as a mechanism to track how audited entities' made changes to their compliance with HIPAA following an OCR audit.

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does it Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

 OIGatHHS

 HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov