Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

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

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

Thomas M. Salmon
Assistant Inspector General

November 2013
A-04-11-05025

Office of Inspector General

https://oig.hhs.gov

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

Office of Audit Services

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

Office of Evaluation and Inspections

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

Office of Investigations

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

Office of Counsel to the Inspector General

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

Notices

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

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

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

EXECUTIVE SUMMARY

BACKGROUND

Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the U.S. Department of Health and Human Services (HHS) to develop national standards for the use and dissemination of health care information, including standards to protect electronic protected health information (ePHI). To satisfy that requirement, HHS published the HIPAA Security Rule (Security Rule), which describes the administrative, physical, and technical safeguards necessary to ensure the confidentiality, integrity, and availability of ePHI.

Health Information Technology for Economic and Clinical Health Act

As part of the American Recovery and Reinvestment Act of 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH extends the Security Rule and its civil penalties for covered entities that do not comply with the Security Rule to business associates of covered entities. HITECH also requires HHS to provide for periodic audits of covered entities to ensure their compliance with HIPAA requirements.

Prior Office of Inspector General Reports on Oversight of the Security Rule

In October 2008, we reported to the Centers for Medicare & Medicaid Services (CMS) that it had taken limited actions to ensure covered entities complied with the Security Rule. At the time of our 2008 report, CMS had not conducted Security Rule compliance audits of covered entities and had not established policies or procedures for conducting those audits. We recommended that CMS establish policies and procedures for conducting compliance audits of covered entities.

In our May 2011 report to the Office for Civil Rights (OCR) (after the delegation of responsibility for the Security Rule to OCR in 2009), we summarized the results of our audits of CMS's oversight and enforcement of Security Rule implementation at seven hospitals. The report disclosed numerous control weaknesses at the hospitals and demonstrated the need for greater OCR oversight and enforcement. We also reported that, in 2009, CMS began conducting self-initiated compliance audits of covered entities. We recommended that OCR continue the compliance-audit process that CMS had begun and implement procedures for conducting compliance reviews.

OBJECTIVES

Our objectives were to determine whether: (1) OCR met Federal requirements for oversight and enforcement of the Security Rule and (2) OCR's computer systems used to oversee and enforce the Security Rule met Federal cybersecurity requirements.

SUMMARY OF FINDINGS

OCR met some Federal requirements for oversight and enforcement of the Security Rule. OCR made available to covered entities guidance that promoted compliance with the Security Rule and OCR established an investigation process for responding to reported violations of the Security Rule. 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:

- 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.

- Although OCR established an investigation process for responding to reported violations of the Security Rule, its Security Rule investigation files did not contain required documentation supporting key decisions because its staff did not consistently follow OCR investigation procedures by sufficiently reviewing investigation case documentation. OCR had not implemented sufficient controls, including supervisory review and documentation retention, to ensure investigators follow investigation policies and procedures for properly initiating, processing, and closing Security Rule investigations.

In addition, OCR had not fully complied with Federal cybersecurity requirements included in the National Institute of Standards and Technology (NIST) *Risk Management Framework* for its information systems used to process and store investigation data because it focused on system operability to the detriment of system and data security. For example, OCR did not obtain HHS authorizations to operate the three systems used to oversee and enforce the Security Rule. In addition, it did not complete privacy impact assessments, risk analyses, or system security plans for two of the three systems. Exploitation of system vulnerabilities, normally identified through the Risk Management process, could impair OCR's ability to perform functions vital to its mission.

RECOMMENDATIONS

We recommend that OCR:

- assess the risks, establish priorities, and implement controls for its HITECH auditing requirements;

- provide for periodic audits in accordance with HITECH to ensure Security Rule compliance at covered entities;

- implement sufficient controls, including supervisory review and documentation retention, to ensure policies and procedures for Security Rule investigations are followed; and
- implement the NIST *Risk Management Framework* for systems used to oversee and enforce the Security Rule.

OFFICE FOR CIVIL RIGHTS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In its comments on our draft report, OCR generally concurred with our recommendations and described the actions it has taken to address them. In one of its comments, OCR stated that it had contracted for the development of its audit mandate options, had developed an audit protocol, had conducted pilot audits of covered entities, and was evaluating the results of its pilot audit program. However, OCR explained that no funds had been appropriated for it to maintain a permanent audit program and that funds used to support audit activities previously conducted were no longer available. OCR also provided technical comments, which we addressed as appropriate.

We remain concerned about OCR's ability to comply with the HITECH audit requirement and the resulting limited assurance that ePHI is secure at covered entities because of OCR's comment regarding limited funding resources for its audit mandates. Furthermore, in response to one of OCR's technical comments, we changed our report language to clarify our finding on OCR's oversight and enforcement of covered entity compliance with the Security Rule by removing a reference to Security Rule requirements. Although the Security Rule authorized compliance reviews of covered entities in 2006 by stating that OCR "may conduct compliance reviews to determine" Security Rule compliance, HITECH changed the requirement in 2009 to state that OCR "shall provide for periodic audits to ensure" Security Rule compliance.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. No. 104-191) required the U.S. Department of Health and Human Services (HHS) to develop national standards for the use and dissemination of health care information, including standards to protect electronic protected health information (ePHI). These standards are applicable to the three types of covered entities: health plans, healthcare clearinghouses, and certain healthcare providers.

To satisfy the requirement to develop national standards to protect ePHI, HHS published the HIPAA Security Rule (Security Rule) in 45 CFR parts 160, 162, and 164. The Security Rule describes the administrative, physical, and technical safeguards necessary to ensure the confidentiality, integrity, and availability of ePHI.

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 Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH extended the Security Rule and related civil penalties to business associates of covered entities.[1] HITECH also requires HHS to provide for periodic audits of covered entities to ensure compliance with HIPAA requirements (subtitle D, part 1, § 13411**)**.

Delegation of Authority To Administer the Health Insurance Portability and Accountability Act of 1996 Security Rule

On October 7, 2003, HHS delegated to the Centers for Medicare & Medicaid Services (CMS) the authority to enforce compliance with the Security Rule and to impose civil monetary penalties on covered entities that violate it. The Final Rule for enforcement of the Security Rule became effective on March 16, 2006 (71 Fed. Reg. 8390 (Feb. 16, 2006)).

On July 27, 2009, HHS delegated the authority for the oversight and enforcement of the Security Rule to the Office for Civil Rights (OCR).

Responsibilities of the Office for Civil Rights

As HHS's civil rights, health information privacy, and security enforcement division, OCR's purpose is to protect fundamental rights of nondiscrimination and ensure compliance with health information privacy and security laws. As of July 27, 2009, OCR became responsible for ensuring that covered entities comply with the Security Rule and for investigating and resolving potential HIPAA violations. The HITECH Act requires OCR to provide for periodic audits of

[1] In this audit report, we used the term "covered entities" also to refer to the business associates of covered entities.

covered entities, while Federal regulations grant OCR the leeway to resolve matters involving indications of noncompliance informally[2] or to impose civil monetary penalties if it determines that a covered entity has violated a Security Rule requirement. OCR is also required to comply with Federal internal control and cybersecurity requirements.

Prior Office of Inspector General Reports on Oversight of the Security Rule

In October 2008, we reported to CMS[3] that it had taken limited actions to ensure that covered entities complied with the requirements of the Security Rule. At the time of our report, CMS had not conducted any Security Rule compliance audits of covered entities and had not established any policies or procedures for conducting them. We recommended that CMS establish policies and procedures for conducting compliance audits of covered entities.

In a May 2011 report to OCR,[4] we summarized the results of our reviews of CMS's oversight and enforcement of Security Rule implementation at seven hospitals located in California, Georgia, Illinois, Massachusetts, Missouri, New York, and Texas. The report disclosed numerous control weaknesses at the hospitals and demonstrated the need for greater OCR oversight and enforcement. We also reported that, in 2009, CMS began conducting self-initiated compliance audits of covered entities. We recommended that OCR continue the compliance audit process that CMS had begun and implement procedures for conducting compliance audits to ensure that Security Rule controls are in place and operating as intended to protect ePHI at covered entities.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Our objectives were to determine whether: (1) OCR met Federal requirements for oversight and enforcement of the Security Rule and (2) OCR's computer systems used to oversee and enforce the Security Rule met Federal cybersecurity requirements.

Scope

We performed our fieldwork at OCR's headquarters in Washington, DC, and its Atlanta regional office. We assessed OCR's Security Rule oversight and enforcement for the period July 2009 through May 2011 and its computer systems as of May 2011.

[2] "Informal means" may include demonstrated compliance, a completed corrective action plan, or other agreements (45 CFR § 160.312).

[3] On October 27, 2008, we issued a report to CMS entitled *Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance and Portability and Accountability Act of 1996 Oversight* (A-04-07-05064).

[4] On May 16, 2011, we issued a report to OCR entitled *Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight* (A-04-08-05069).

Methodology

To accomplish our objectives, we:

- reviewed Federal laws and regulations pertaining to ePHI and cybersecurity;

- reviewed OCR's policies, processes, systems, and applications used to oversee and enforce the Security Rule;

- assessed OCR's oversight and enforcement of the Security Rule as applied to covered entities;

- evaluated the risk assessment OCR used to allocate its oversight and enforcement resources;

- reviewed OCR's use of civil monetary penalties for Security Rule violations;

- interviewed OCR staff members in Washington, D.C.; Atlanta, Georgia; Boston, Massachusetts; Chicago, Illinois; and Philadelphia, Pennsylvania; to understand their interpretation of and processes for implementing and enforcing the Security Rule;

- assessed OCR's guidance to covered entities regarding the Security Rule;

- reviewed OCR's contracts and interviewed contractor personnel who performed technical analyses and provided recommendations to OCR regarding potential Security Rule violations;

- judgmentally selected 30 closed and 30 open investigations from 364 investigations of potential Security Rule violations conducted between July 2009 and February 2011; and

- interviewed the OCR official responsible for overseeing investigations and supervising regional OCR staff.

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.

FINDINGS AND RECOMMENDATIONS

OCR met some Federal requirements for oversight and enforcement of the Security Rule:

- OCR made available to covered entities guidance to promote compliance with the Security Rule.

- OCR established an investigation process for responding to reported violations of the Security Rule.

- OCR followed Federal regulations for penalizing Security Rule violators. It closed 147 of 364 Security Rule investigations from July 2009 through February 2011. Although OCR might have been able to impose civil monetary penalties for some of the most severe violations, OCR followed Federal requirements by resolving those cases informally.

However, OCR did not meet other Federal requirements for the oversight and enforcement of the Security Rule:

- Although OCR made available to covered entities guidance to promote 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.

- Although OCR established an investigation process for responding to reported violations of the Security Rule, its Security Rule investigation files did not contain required documentation supporting key decisions made during those investigations because its staff did not consistently follow OCR investigation procedures by sufficiently reviewing investigation case documentation. OCR had not implemented sufficient controls, including supervisory review and documentation retention, to ensure investigators follow investigation policies and procedures for properly initiating, processing, and closing Security Rule investigations. By not consistently following its investigation procedures and reviewing case documentation, OCR had limited assurance that it had identified and mitigated vulnerabilities to ePHI during Security Rule investigations.

In addition, OCR had not fully complied with Federal cybersecurity requirements included in the National Institute of Standards and Technology (NIST) *Risk Management Framework* for its information systems used to process and store investigation data because it focused on system operability to the detriment of system and data security. For example, OCR did not obtain HHS authorizations to operate the three systems used to oversee and enforce the Security Rule. In addition, it did not complete privacy impact assessments, risk analyses, and system security plans for two of the three systems. Exploitation of unaddressed system vulnerabilities normally identified through the Risk Management process, could impair OCR's ability to perform functions vital to its mission.

OFFICE FOR CIVIL RIGHTS PARTIALLY MET REGULATORY REQUIREMENTS FOR OVERSIGHT AND ENFORCEMENT

Periodic Audits Not Provided For

HITECH requires OCR to provide for periodic audits to ensure that covered entities and their business associates comply with Security Rule requirements (HITECH Act, section 13411). The Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*, requires management to establish and maintain controls to comply with applicable laws and regulations. It further states that management should perform risk assessments to identify the most significant areas in which to place or enhance controls.

OCR did not provide for periodic audits of covered entities in accordance with these Federal requirements. Instead, OCR continued to follow the complaint-driven approach developed jointly by CMS and OCR but discontinued the compliance-audit process that CMS had begun in 2009.

OCR had not established controls for complying with HITECH's auditing requirements. For example, OCR had not assessed which entities or what systems used for storing or processing ePHI presented the greatest risk of ePHI exposure. Instead of assessing the risks, establishing priorities, and implementing controls for the redelegated Security Rule and the HITECH requirements, OCR applied the resources and procedures it had been using for its responsibilities in civil rights and health privacy oversight and enforcement before the redelegation.

OCR allocated its resources to manage an increasing number of Security Rule investigations originating primarily from press reports, reported breaches affecting 500 or more individuals, and complaints from the public. OCR officials stated that OCR did not have sufficient resources to expand its compliance efforts beyond event-driven compliance investigations. In addition, OCR did not have the expertise needed to meet its Security Rule and HITECH responsibilities, which include the ability to audit security controls for systems that process and store ePHI.[5]

Because OCR did not perform the compliance audits mandated by HITECH, it had limited information about the status of Security Rule compliance at covered entities. Therefore, it had limited assurance that ePHI was secure and might have missed opportunities to motivate covered entities to strengthen ePHI security. The cumulative results of an audit program would also have helped OCR better understand the areas in which ePHI was vulnerable and might have helped OCR develop more effective ways to allocate its oversight resources.

Insufficient Records for Security Rule Investigations

OCR's publication, *Dual Process Complaint Manual: The Process and Workflow for Security Rule and Dual Process Complaints*, requires designated OCR headquarters and regional personnel to update the Compliance Data System (CDS) as needed with all documentation

[5] An evaluation of budget and staffing to determine whether OCR had sufficient resources and staff expertise to meet its responsibilities was outside the scope of this review. Therefore, we have not made any recommendations to address the issues raised by OCR officials.

required to initiate, process, and close Security Rule investigations. OMB Circular A-123 requires management to establish and maintain controls to achieve the objectives of effective and efficient operations.

Security Rule investigation records did not contain documentation needed to support key decisions made during those investigations. Specifically, 39 of 60 selected records were missing 1 or more of the documents necessary to initiate, process, or close those investigations. Examples of missing documentation included initial complaint documents, closure letters, and documents required for tracking complaint status through the Security Rule investigation process.

OCR Security Rule investigation records were missing documentation because OCR investigators did not consistently follow OCR's policies and procedures for documenting case investigations and OCR management did not implement sufficient controls, such as supervisory reviews, to ensure that the investigators did so.

Without adequate supporting documentation for tracking investigations, such as initial complaint and case progress-tracking forms, OCR management could not be certain that its investigators conducted Security Rule investigations properly. In addition, OCR management could not be certain that it identified and mitigated problems related to the initial complaints during the investigation process. Without a closure letter, OCR management could not be certain that OCR had approved a covered entity's mitigation strategy.

SYSTEMS DID NOT FULLY COMPLY WITH FEDERAL CYBERSECURITY REQUIREMENTS

The Federal Information Security Management Act of 2002 (FISMA) requires each Federal agency to develop, document, and implement an agencywide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. HHS requires its operating and staff divisions to follow FISMA and other Federal cybersecurity requirements for the secure development, operation, and maintenance of information systems. More specifically, HHS requires security authorizations, privacy impact assessments, risk analyses, and system security plans for Federal information systems (*HHS Standard for FISMA Inventory Management*). The detailed requirements are in Appendix A.

OCR's computer systems used to store, retrieve, and track Security Rule oversight and enforcement data did not fully comply with Federal cybersecurity requirements. OCR had not fully implemented the NIST *Risk Management Framework*[6] for three of its Security Rule oversight systems: the Program Information Management System (PIMS), the CDS, and the Breach Notification system. More specifically, OCR did not:

[6] NIST's *Risk Management Framework* provides a structured process and information to help organizations identify the risks to their information systems, assess those risks, and take steps to reduce risks to an acceptable level. Available online at http://csrc.nist.gov/publications/nistbul/july2009_risk-management-framework.pdf. Accessed on July 2, 2012.

- obtain HHS authorizations to operate its PIMS, CDS, or Breach Notification system;
- complete a privacy impact assessment and risk analysis for the CDS or the Breach Notification system;
- develop a system security plan for the CDS and the Breach Notification systems; or
- implement additional Federal security requirements not included above for its Breach Notification system.

In general, OCR management focused on the operability of the systems used for HIPAA oversight and enforcement by its predecessor CMS when OCR was delegated additional Security Rule and HITECH responsibilities and did not focus on securing the systems used to store, retrieve, process, and track Security Rule oversight and enforcement data. OCR copied, renamed, and partially modified the CMS Administrative Simplification Enforcement Tool system into its CDS system to receive, maintain, and process Security Rule investigation data. However, OCR management did not give Federal cybersecurity requirements sufficient priority and, consequently, did not complete *Risk Management Framework* requirements for its PIMS, CDS, or Breach Notification system. Further, the underlying reason OCR's Breach Notification system did not meet Federal cybersecurity requirements was that OCR management had not classified it properly as a system subject to Federal cybersecurity requirements.

Although we found no evidence that anyone had compromised OCR's sensitive information or information systems, by not complying with Federal cybersecurity requirements, OCR increased the risk that it might not identify or mitigate system vulnerabilities. Exploitation of any of those system vulnerabilities could impair OCR's ability to perform various business processes, including compliance activities, real-time access and results reporting, timely responses to complaints, and completion of investigations. It also could increase the risk of unauthorized disclosure or destruction of ePHI.

RECOMMENDATIONS

We recommend that OCR:

- assess the risks, establish priorities, and implement controls for its HITECH auditing requirements;
- provide for periodic audits in accordance with HITECH to ensure Security Rule compliance at covered entities;
- implement sufficient controls, including supervisory review and documentation retention, to ensure policies and procedures for Security Rule investigations are followed; and
- implement the NIST *Risk Management Framework* for systems used to oversee and enforce the Security Rule.

OFFICE FOR CIVIL RIGHTS COMMENTS

In its comments on our draft report, OCR generally concurred with our recommendations and described the actions it has taken to address them. In one of its comments, OCR stated that it had contracted for the development of its audit mandate options, had developed an audit protocol, had conducted pilot audits of covered entities, and was evaluating the results of its pilot audit program. However, OCR explained that no funds had been appropriated for it to maintain a permanent audit program and that funds used to support audit activities previously conducted were no longer available. OCR also provided technical comments, which we addressed as appropriate. OCR's comments, excluding technical comments, are included as Appendix B.

OFFICE OF INSPECTOR GENERAL RESPONSE

We remain concerned about OCR's ability to comply with the HITECH audit requirement and the resulting limited assurance that ePHI is secure at covered entities because of OCR's comment regarding limited funding resources for its audit mandates. Furthermore, in response to one of OCR's technical comments, we changed our report language to clarify our finding on OCR's oversight and enforcement of covered entity compliance with the Security Rule by removing a reference to Security Rule requirements. Although the Security Rule authorized compliance reviews of covered entities in 2006 by stating that OCR "may conduct compliance reviews to determine" Security Rule compliance, HITECH changed the requirement in 2009 to state that OCR "shall provide for periodic audits to ensure" Security Rule compliance.

APPENDIXES

APPENDIX A: FEDERAL REQUIREMENTS AND OFFICE FOR CIVIL RIGHTS PROCEDURES

PERIODIC AUDIT REQUIREMENTS

Before HITECH mandated periodic audits of covered entities and business associates, HIPAA authorized compliance reviews of covered entities.

HHS published the Security Rule, which describes the administrative, physical, and technical safeguards necessary to ensure the confidentiality, integrity, and availability of ePHI. Under the Security Rule:

> The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter (45 CFR § 160.308).

HITECH (section 13411) stipulates that "[t]he Secretary shall provide for periodic audits to ensure that covered entities and business associates ... comply with [Security Rule] requirements."

SECURITY RULE ENFORCEMENT REQUIREMENTS

Federal regulations (45 CFR § 160.402 (a)) state that the Secretary will impose a civil money penalty on a covered entity if the Secretary determines that the covered entity has violated a Security Rule requirement.

Additional regulations (45 CFR § 160.312) state that: "(1) If an investigation of a complaint … or a compliance review … indicates noncompliance, the Secretary will attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance, a completed corrective action plan, or other agreements."

OCR publication *Dual Process Complaint Manual: The Process and Workflow for Security Rule and Dual Process Complaints* (the manual) applies to Security Rule cases. The manual states that designated OCR headquarters and regional personnel will update the Compliance Data System as needed with all documentation required to initiate, process, and close a Security Rule investigation.

INTERNAL CONTROL REQUIREMENTS

OMB Circular No. A-123 states: "[m]anagement is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Management shall consistently apply the internal control standards to meet each of the internal control objectives and to assess internal control effectiveness."

It further states that internal control is a:

> …means of managing the risk associated with Federal programs and operations. Managers should define the control environment (e.g., programs, operations, or financial reporting) and then perform risk assessments to identify the most significant areas within that environment in which to place or enhance internal control. The risk assessment is a critical step in the process to determine the extent of controls. Once significant areas have been identified, control activities should be implemented. Continuous monitoring and testing should help to identify poorly designed or ineffective controls and should be reported upon periodically….

FEDERAL CYBERSECURITY REQUIREMENTS

FISMA requires each Federal agency to develop, document, and implement an agencywide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Federal Information Processing Standards Publication *Minimum Security Requirements for Federal Information and Information Systems* (FIPS 200) requires information systems to comply with the most recent edition of NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems.* FIPS 200 states: "Organizations must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in NIST [SP] 800-53…. Organizations must use the most current version of NIST [SP] 800-53, as amended, for the security control selection process."

The HHS Office of Chief Information Officer (OCIO) policy, *HHS-OCIO Policy for Information Systems Security and Privacy* (HHS-OCIO-2011-0003), section 4, established U.S. Government mandates for the secure development, operation, and maintenance of information systems in HHS and its Operating Divisions/Staff Divisions (OPDIVs/STAFFDIVs).

Sections 4.1.1 and 4.1.2 state:

> OPDIVs/STAFFDIVs shall use NIST … SP 800-37 Revision (Rev.) 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (dated February 2010), as the methodology for the security authorization of information systems (formerly known as "certification and accreditation" or "C&A"), in accordance with FISMA and direction from OMB…. OPDIVs/STAFFDIVs shall comply with Department minimum requirements when preparing security authorization packages for information systems.

NIST SP 800-53, Revision 3, in section CA-2, *Security Assessment*, states:

> The organization:
>
> a. Develops a security assessment plan that describes the scope of the assessment including:
>
> 1) Security controls and control enhancements under assessment;
> 2) Assessment procedures to be used to determine security control effectiveness; and
> 3) Assessment environment, assessment team, and assessment roles and responsibilities;
>
> b. Assesses the security controls in the information system … to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
>
> c. Produces a security assessment report that documents the results of the assessment; and
>
> d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

The HHS Standard for FISMA Inventory Management policy (HHS Inventory Policy) requires all HHS information technology systems to be recorded through the HHS FISMA reporting tool and the following to be documented:

- System type (i.e., GSS [general support system], major application, or minor application)…;

- Information type(s) and corresponding FIPS 199 risk impact levels (i.e., categorizations) for the individual information types and for the IT system;

- Privacy Impact Assessment (PIA);

- e-Authentication risk assessment completion date and highest authentication assurance level; and

- Weaknesses and corrective actions within a POA&M [Plan of Actions and Milestones]. The GSS or major application POA&M must account for the weaknesses of all applications (major or minor, as applicable) within its accreditation boundary.

The HHS Inventory Policy also requires all HHS information technology systems to be certified and accredited in accordance with NIST and HHS guidance. The scope of the certification and accreditation shall be commensurate with the FIPS 199 risk impact level of the system and document a Risk Assessment, Security Assessment Report, POA&M, and accreditation decision letter with corresponding full Authorization to Operate. The scope should also include a current System Security Plan and an Information Technology Contingency Plan.

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems—A Security Life Cycle Approach*, revision 1, section 2.1, states that, to fulfill the Risk Management Framework, organizations must:

- Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.

- Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

- Implement the security controls and describe how the controls are employed within the information system and its environment of operation.

- Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

- Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

APPENDIX B: OFFICE FOR CIVIL RIGHTS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

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

September 26, 2013

MEMORANDUM

TO: Thomas M. Salmon
Assistant Inspector General for Audit Services

FROM: Leon Rodriguez
Director

SUBJECT: 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)

Thank you for the opportunity to review the subject draft report. The Office for Civil Rights (OCR) appreciates the efforts and recommendations of the Office of the Inspector General (OIG). As detailed below, OCR has made significant progress in addressing the recommendations in the draft report. [redacted]

- [redacted]

- [redacted]

Office of Inspector General Note - Technical comments in the auditee's response to the draft have been omitted from the final report and all appropriate changes have been made.

[redacted]

- [redacted]

- [redacted]

Responses to Recommendations:

1) Assess the risks, establish priorities, and implement controls for its Security Rule and HITECH requirements

The Office for Civil Rights (OCR) has developed and executed a series of strategic initiatives to implement the Security Rule and HITECH requirements. OCR was a partner in the development of HHS's Federal Health IT Strategic Plan for 2011-2015, which describes the Federal government's strategy to implement the HITECH Act's initiatives across the Department with a goal toward improving health and health care for all Americans through use of health information and technology. Goal III of the Federal Health IT Strategic Plan focuses on Federal privacy and security efforts so that electronic health information will be protected and used appropriately within health IT systems in patient care.

OCR issued final rules in January 2013 to implement modifications to the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, Breach Notification, and Enforcement Rules, as required by the HITECH Act. This rule effectively extends the use and disclosure requirements of the Privacy Rule, as well as the provisions of the Security Rule to the contractors of health care providers and health plans ("business associates") covered by HIPAA, as well as their subcontractors.

OCR has enhanced enforcement of the HIPAA Rules. From 2008 through 2012, OCR obtained corrective action from covered entities in more than 13,000 cases in which our investigations found indications of noncompliance with HIPAA. During the same period, OCR reached resolution agreements with covered entities in 11 cases. The payments resulting from these 11 resolution agreements total approximately $10 million. OCR has also imposed a civil monetary penalty of about $4 million in one case in which the covered entity failed for up to a year and a half to provide 41 individuals with access to their health information, as required by the HIPAA Privacy Rule, and failed to cooperate with OCR's investigation.

Office of Inspector General Note - Technical comments in the auditee's response to the draft have been omitted from the final report and all appropriate changes have been made.

OCR continues to develop privacy and security-oriented technical assistance materials for HIPAA covered entities and business associates:

- OCR developed guidance to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure e-PHI through conducting a risk analysis of their information systems that handle e-PHI.
- OCR provided technical assistance in the development of the NIST HIPAA Security Toolkit Application, a self-assessment survey intended to help organizations better understand the requirements of the HIPAA Security Rule.
- ONC and OCR partnered to develop tools and resources to help providers meet privacy and security requirements addressing the security of ePHI when using mobile devices and developed a videogame that provides privacy and security training for health care professionals.
- OCR has developed 2 educational videos that raise awareness about safeguarding electronic health information and the requirements of the Security Rule. These videos are available through the "You Tube" Internet website.
- OCR has developed video training modules that provide health care professionals and staff with information on the requirements of the Security Rule, the importance of conducting an information security risk analysis, and the importance of safeguarding mobile devices. These video titles are available on the Medscape Internet website.

2) Provide for periodic audits in accordance with HITECH to ensure Security Rule compliance at covered entities

Section 13411 of the HITECH Act states that the Department shall provide for periodic audits of covered entities and business associates that are subject to the requirements of the HITECH Act and the HIPAA Rules to ensure compliance with such requirements. Since 2010, OCR has made significant strides to develop and implement an audit program to ensure the compliance of covered entities and business associates with the HIPAA Privacy, Security, and Breach Notification Rules. OCR has contracted for the development of options for implementation of the audit mandate, developed a comprehensive audit protocol that also serves as a guide for entity compliance, conducted 115 audits of covered entities, and initiated an evaluation of the audit program conducted to date to inform decision making about future audits. While OCR agrees with the recommendation that the HITECH audit program represents an effective tool, no monies have been appropriated for OCR to maintain a permanent audit program. [1]

Audit Plan Development
In 2010, OCR contracted with Booz Allen Hamilton (BAH) to identify key issues that OCR would need to address in the development and operation of an audit program and to recommend

[1] OCR used ARRA funds to support the audit activities described. The availability of these funds expired in December 2012.

models for conducting audits. BAH reviewed existing audit programs and industry materials, and conducted interviews with industry experts. The BAH report addressed the phases of an audit program, from planning to reporting and follow-up, and identified a number of key issues and decisions that OCR would need to address prior to beginning audits.

Based upon the model options and issues identified by BAH, OCR decided to pursue a pilot audit strategy, which included establishing the building blocks for an audit program, conducting comprehensive audits in an iterative manner to leverage the experiences of initial audits to benefit later audits, and contracting out the performance of the onsite audits. At the same time, OCR committed to an evaluation of the pilot audit experience.

Building the Audit Program

Prior to conducting any audit, OCR needed to identify the universe of covered entities[2] that would be subject to audits and to develop an audit protocol. To identify covered entities, OCR contracted with BAH to develop a comprehensive listing of covered entities from existing public and private data sources. To develop the protocol to use for audits of covered entities, OCR contracted with KPMG. Both the listing of covered entities and the HIPAA audit protocol were completed in 2011.

Conducting Audits

OCR decided that the most effective strategy to start the audit program was to contract for onsite audits to be performed by a single entity, and to first test the protocol on a small, diverse group of covered entities with later expansion to a larger group of covered entities. OCR's goal was to identify a baseline for covered entity compliance among a broad section of the HIPAA Privacy, Security, and Breach Notification standards while gaining the knowledge and experience in the operation of an audit function.

OCR selected 50 standards from across the three Rules for assessment. The focus in the audits was to assess whether entities had sufficient policies, procedures, and infrastructure in place to meet the HIPAA Rule requirements. Between December 2011 and March 2012, KPMG conducted 20 audits. Based upon the initial audit experience and use of the protocol, changes were made to the protocol and to the audit process. KPMG then conducted a final 95 audits of various sizes and types of covered entities from April 2012 to December 2012.

Of the 115 audits conducted, 47 health plans, 61 health care providers, and 7 clearinghouses were audited. The covered entities audited included a broad mix of public and private entities, local, regional and national entities, and entities with both significant and minor health information technology adoption.

The audit results demonstrated several clear trends. Although Security Rule standards represented one quarter of standards assessed by KPMG, findings and observations for those

[2] Note that because final regulations for the compliance obligations of business associates were not yet in place, OCR focused on auditing covered entities in the pilot phase of the audit program.

standards accounted for over half of all findings and observations. In addition, although thirteen entities had no findings or observations, health care providers generally had greater compliance gaps than health plans and clearinghouses. Finally, small entities overall struggled in each assessment area – privacy, security and breach notification – while larger entities had proportionally fewer and more limited findings.

Evaluation of the Pilot Audit Program
Following the completion of audits by KPMG in 2012, OCR contracted with Price Waterhouse Coopers (PWC) to evaluate a variety of aspects of the pilot HIPAA audit program, including the selection of entities and standards, audit conclusions and work papers, and the operation and management of the program by OCR. The evaluation will include a survey of all audited entities to assess the impact of the audits on the industry and covered entities individually. Final recommendations will be made to OCR in the last quarter of 2013.

Based upon the findings and recommendations of PWC's evaluation, OCR will make decisions about a permanent audit program. Future decisions will include the strategy and process for audits of business associates and a development of program priorities. Future audits are less likely to be broad assessments generally across the Rules and more likely to focus on key areas of concern for OCR identified by new initiatives, enforcement concerns, and Departmental priorities.

3) Implement sufficient controls, such as supervisory reviews and documentation retention to ensure policies and procedures in Security Rule investigations are followed.

OIG found that there were insufficient records of the documentation of complaint investigations and compliance reviews in the Compliance Data System (CDS) information system that OCR used to manage and store the documentation for the investigation of HIPAA Security Rule complaints and compliance reviews. At the time of OIG's review, OCR operated two information systems to support and track investigations, as well as other official correspondence of the agency. The Compliance Data System (CDS) was used to support the activities related to the enforcement activities of the Security Rule. The Program Information Management System (PIMS) was used as the information system to support all of OCR's other administrative and enforcement activities. In 2012, OCR merged the data from CDS into PIMS to improve efficiency and assure that the documentation of Security Rule complaint investigations and compliance reviews were accurate and complete. CDS has been decommissioned and PIMS now serves as the only information system to manage the documentation and case progression of OCR's activities to support the Security Rule.

OCR made a significant upgrade to its PIMS information systems that implemented specific requirements that ensure all cases have the appropriate documentation, including initiating and closing documentation, and management review. Depending on the type of case, additional information may be required. Any case that is investigated will have a strategy in the case folder which is approved by management. Investigators on Security Rule cases have access to subject matter experts with appropriate technical certifications for assistance in analyzing and evaluating information security issues. Management reviews of case evidence, procedural documentation, and investigative procedures are recorded in PIMS for all closures.

4) Implement the NIST Risk Management Framework for system used to oversee and enforce the Security Rule.

OIG found that information systems used by OCR for its oversight and enforcement data did not fully comply with the Federal cybersecurity requirements. Since the OIG review, OCR has taken steps to assure its compliance with the HHS Standards for FISMA Inventory Management:

- CDS has been decommissioned and all data has been merged into PIMS. All hardware and software associated with CDS has been decommissioned in accordance with the procedures of the hosting facility at NIH/CIT.
- PIMS has been brought into compliance with the FISMA requirements for completing a privacy impact assessment, risk analysis and system security plan. An authorization to operate (ATO) PIMS was issued by the Department's Chief Information Officer and is valid through January 2015.
- Administrative and technical management of the Breach Notification System is the responsibility of the Assistant Secretary for Public Affairs (ASPA). ASPA advises that the system operates under an ATO granted for its managed network systems.

OCR would be pleased to provide the documentation in support of these activities on request.

Thank you again for the opportunity to review the draft report. Please do not hesitate to contact me with any questions.