



OCT 27 2008

Washington, D.C. 20201

TO: Kerry Weems
Acting Administrator
Centers for Medicare & Medicaid Services

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

SUBJECT: Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight (A-04-07-05064)

The attached final report provides the results of our review of the Centers for Medicare & Medicaid Services (CMS) oversight and enforcement of covered entities' implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

On August 21, 1996, Congress enacted HIPAA (P.L. No. 104-191). HIPAA established national standards that protect the confidentiality and integrity of electronic protected health information (ePHI) while it is being stored or transmitted between entities. The HIPAA Administrative Simplification was added to the Social Security Act. The HIPAA Security Rule is a component of the HIPAA Administrative Simplification security standards.

On October 7, 2003, the U.S. Department of Health and Human Services delegated to CMS: (1) the authority and responsibility to interpret, implement, and enforce the HIPAA Security Rule provisions; (2) the authority to conduct compliance reviews and to investigate and resolve complaints of HIPAA Security Rule noncompliance; and (3) the authority to impose civil monetary penalties for a covered entity's failure to comply with the HIPAA Security Rule provisions. The Final Rule for enforcement of this delegation became effective on February 16, 2006.

Our objective was to evaluate the effectiveness of CMS's oversight and enforcement of covered entities' implementation of the HIPAA Security Rule.

CMS had taken limited actions to ensure that covered entities adequately implement the HIPAA Security Rule. These actions had not provided effective oversight or encouraged enforcement of the HIPAA Security Rule by covered entities. Although authorized to do so by Federal regulations as of February 16, 2006, CMS had not conducted any HIPAA Security Rule compliance reviews of covered entities. To fulfill its oversight responsibilities, CMS relied on complaints to identify any noncompliant covered entities that it might investigate. As a result,

CMS had no effective mechanism to ensure that covered entities were complying with the HIPAA Security Rule or that ePHI was being adequately protected.

Although reliance on complaints alone was ineffective for identifying noncompliant covered entities, we noted that CMS had an effective process for receiving, categorizing, tracking, and resolving complaints. CMS has developed and implemented detailed procedures for receiving complaints, communicating with filed-against entities, coordinating with the Office for Civil Rights for complaints with privacy elements, developing corrective action plans, and remediating complaints.

Ongoing Office of Inspector General audits of various hospitals nationwide indicate that CMS needs to become more proactive in overseeing and enforcing implementation of the HIPAA Security Rule by focusing on compliance reviews. Preliminary results of these audits show numerous, significant vulnerabilities in the systems and controls intended to protect ePHI at covered entities. These vulnerabilities place the confidentiality and integrity of ePHI at high risk. During our audit, CMS began taking steps to conduct compliance reviews. After we completed our fieldwork but before we issued our report, CMS executed a contract to conduct compliance reviews at covered entities.

We recommend that CMS establish policies and procedures for conducting HIPAA Security Rule compliance reviews of covered entities.

CMS did not agree with our findings because it believes that its complaint-driven enforcement process has furthered the goal of voluntary compliance. CMS agreed, however, that compliance reviews are a useful enforcement tool as part of a more comprehensive enforcement strategy. CMS agreed with our recommendation to establish specific policies and procedures for conducting compliance reviews of covered entities but emphasized that compliance reviews are just one of several tools that can be used to promote compliance.

Although CMS's complaint-driven enforcement process has furthered the goal of voluntary compliance, the significant vulnerabilities we identified at hospitals throughout the country would not generally have been identified in HIPAA Security Rule complaints. In fact, CMS has received very few complaints regarding potential HIPAA Security Rule violations. Including compliance reviews of covered entities to its oversight process will enhance CMS's ability to determine whether the HIPAA Security Rule is being properly implemented.

Pursuant to the principles of the Freedom of Information Act, 5 U.S.C. § 552, as amended by P.L. No. 104-231, Office of Inspector General reports generally are made available to the public to the extent the information is not subject to exemptions in the Act (45 CFR part 5). Accordingly, the final report will be posted on the Internet at <http://oig.hhs.gov>.

If you have any questions or comments about this report, please do not hesitate to call me, or your staff may contact Lori S. Pilcher, Assistant Inspector General for Grants, Internal Activities, and IT Audits, at (202) 619-1175 or through e-mail at Lori.Pilcher@oig.hhs.gov or

Peter J. Barbera, Regional Inspector General for Audit Services, Region IV, at (404) 562-7750 or through e-mail at Peter.Barbera@oig.hhs.gov. Please refer to report number A-04-07-05064 in all correspondence.

Attachment

cc:

Wynethea N. Walker
Director, Audit Liaison Staff
Centers for Medicare & Medicaid Services

Anthony Trenkle
Director, Office of E-Health Standards and Services
Centers for Medicare & Medicaid Service

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

**NATIONWIDE REVIEW OF THE
CENTERS FOR MEDICARE &
MEDICAID SERVICES HEALTH
INSURANCE PORTABILITY AND
ACCOUNTABILITY ACT OF 1996
OVERSIGHT**



Daniel R. Levinson
Inspector General

October 2008
A-04-07-05064

Office of Inspector General

<http://oig.hhs.gov>

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

Office of Audit Services

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

Office of Evaluation and Inspections

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

Office of Investigations

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

Office of Counsel to the Inspector General

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

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at <http://oig.hhs.gov>

Pursuant to the principles of the Freedom of Information Act, 5 U.S.C. § 552, as amended by Public Law 104-231, Office of Inspector General reports generally are made available to the public to the extent the information is not subject to exemptions in the Act (45 CFR part 5).

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

On August 21, 1996, Congress enacted P.L. No. 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Sections 261 and 262 of HIPAA established national standards that protect the confidentiality and integrity of electronic protected health information (ePHI) while it is being stored or transmitted between entities.

The HIPAA Administrative Simplification was added to the Social Security Act (the Act) in sections 1171 through 1179. The HIPAA Security Rule is a component of the HIPAA Administrative Simplification security standards and is integrated into 45 CFR parts 160, 162, and 164. Both the Act and the HIPAA Security Rule require a covered entity, such as a health plan or health care provider that transmits any health information in electronic form (45 CFR § 160.103(3)), to (1) ensure the integrity and confidentiality of the information, (2) protect against any reasonably anticipated threats or risks to the security or integrity of the information, and (3) protect against unauthorized uses or disclosures of the information (HIPAA, P.L. No. 104-191, § 262, 45 CFR part 164, subpart C).

On October 7, 2003, the Department of Health and Human Services delegated to the Centers for Medicare & Medicaid Services (CMS) (1) the authority and responsibility to interpret, implement, and enforce the HIPAA Security Rule provisions; (2) the authority to conduct compliance reviews and to investigate and resolve complaints of HIPAA Security Rule noncompliance; and (3) the authority to impose civil monetary penalties for a covered entity's failure to comply with the HIPAA Security Rule provisions. The Final Rule for enforcement of this delegation became effective on February 16, 2006.

The Office of E-Health Standards and Services developed and published HIPAA Security Rule regulations and guidance materials for covered entities. An example is the March 25, 2005, Federal Register notice on how to file a complaint (70 Fed. Reg. 15329). The Office of E-Health Standards and Services also published a series of security papers to give covered entities insight into the HIPAA Security Rule and assistance with implementation of the security standards.

OBJECTIVE

Our objective was to evaluate CMS's oversight and enforcement of covered entities' implementation of the HIPAA Security Rule.

SUMMARY OF FINDINGS

CMS had taken limited actions to ensure that covered entities adequately implement the HIPAA Security Rule. These actions had not provided effective oversight or encouraged enforcement of the HIPAA Security Rule by covered entities. Although authorized to do so by Federal regulations, CMS had not conducted any HIPAA Security Rule compliance reviews of covered entities. To fulfill its oversight responsibilities, CMS relied on complaints to identify any noncompliant covered entities that it might investigate. As a result, CMS had no effective

mechanism to ensure that covered entities were complying with the HIPAA Security Rule or that ePHI was being adequately protected.

Although reliance on complaints alone was ineffective for identifying noncompliant covered entities, we noted that CMS had an effective process for receiving, categorizing, tracking, and resolving complaints. CMS had developed and implemented detailed procedures for receiving complaints, communicating with filed-against entities, coordinating with the Office for Civil Rights for complaints that potentially violate both the HIPAA Security and Privacy Rules, developing corrective action plans, and remediating complaints.

Our ongoing audits of various hospitals nationwide indicate that CMS needs to become proactive in overseeing and enforcing implementation of the HIPAA Security Rule by focusing on compliance reviews. Preliminary results of these audits show numerous, significant vulnerabilities in the systems and controls intended to protect ePHI at covered entities. These vulnerabilities place the confidentiality and integrity of ePHI at high risk. During our audit, CMS began taking steps to conduct compliance reviews. After we completed our fieldwork but before we issued our report, CMS executed a contract to conduct compliance reviews at covered entities.

RECOMMENDATION

We recommend that CMS establish policies and procedures for conducting HIPAA Security Rule compliance reviews of covered entities.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

CMS did not agree with our findings because it believes that its complaint-driven enforcement process has furthered the goal of voluntary compliance. CMS agreed, however, that compliance reviews are a useful enforcement tool as part of a more comprehensive enforcement strategy that also includes complaint investigation and resolution, outreach, education, and working closely with industry to identify and correct security issues.

CMS agreed with our recommendation to establish specific policies and procedures for conducting compliance reviews of covered entities but emphasized that compliance reviews are just one of several tools that can be used to promote compliance as part of a comprehensive enforcement strategy. CMS's comments are included in their entirety in the Appendix.

Although CMS's complaint-driven enforcement process has furthered the goal of voluntary compliance, the significant vulnerabilities we identified at hospitals throughout the country would not generally have been identified in HIPAA Security Rule complaints. In fact, CMS has received very few complaints regarding potential HIPAA Security Rule violations. Including compliance reviews of covered entities in its oversight process will enhance CMS's ability to determine whether the HIPAA Security Rule is being properly implemented.

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
BACKGROUND	1
Delegation of Authority To Administer the Health Insurance Portability and Accountability Act of 1996 Security Rule	1
Office of E-Health Standards and Services	1
OBJECTIVE, SCOPE, AND METHODOLOGY	2
Objective	2
Scope.....	2
Methodology	3
FINDINGS AND RECOMMENDATION	3
FEDERAL AUTHORITIES RELATING TO ENFORCEMENT OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 SECURITY RULE	4
LIMITED ACTION TO ENSURE COMPLIANCE	5
COMPLIANCE REVIEW PROCEDURES NOT ESTABLISHED	5
ELECTRONIC PROTECTED HEALTH INFORMATION AT RISK	5
RECOMMENDATION	5
CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS	6
OFFICE OF INSPECTOR GENERAL RESPONSE	6
APPENDIX	
CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS	

INTRODUCTION

BACKGROUND

On August 21, 1996, Congress enacted P.L. No. 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Sections 261 and 262 of HIPAA established national standards that protect the confidentiality and integrity of electronic protected health information (ePHI) while it is being stored or transmitted between entities.

The HIPAA Administrative Simplification was codified in sections 1171 through 1179 of the Social Security Act (the Act). The HIPAA Security Rule is a component of the HIPAA Administrative Simplification security standards and is integrated into 45 CFR parts 160, 162, and 164. Both the Act and the HIPAA Security Rule require a covered entity, defined as a health plan, health care clearinghouse, or health care provider that transmits any health information in electronic form (45 CFR § 160.103(3)) to (1) ensure the integrity and confidentiality of the information, (2) protect against any reasonably anticipated threats or risks to the security or integrity of the information, and (3) protect against unauthorized uses or disclosures of the information (HIPAA, P.L. No. 104-191, § 262, 45 CFR part 164, subpart C).

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

On October 7, 2003, the Department of Health and Human Services (HHS) delegated to the Centers for Medicare & Medicaid Services (CMS) (1) the authority and responsibility to interpret, implement, and enforce the HIPAA Security Rule provisions; (2) the authority to conduct compliance reviews and to investigate and resolve complaints of HIPAA Security Rule noncompliance; and (3) the authority to impose civil monetary penalties for a covered entity's failure to comply with the HIPAA Security Rule provisions. The Final Rule for enforcement of this delegation became effective on February 16, 2006.

Office of E-Health Standards and Services

To bring together its responsibilities under HIPAA, including enforcement, CMS created a new office in 2002 that later became known as the Office of E-Health Standards and Services (OEES). Some of the functions for which CMS created OEES included:

- developing regulations and guidance materials and providing technical assistance on the HIPAA Administrative Simplification provisions for transactions, code sets, identifiers, and security;
- developing and implementing the enforcement program for HIPAA Administrative Simplification provisions; and
- developing and implementing an outreach program for HIPAA Administrative Simplification provisions by formulating and coordinating a public relations campaign,

preparing and delivering presentations and speeches, responding to inquiries on HIPAA issues, and maintaining liaison with industry representatives.

OESS developed and published HIPAA Security Rule regulations and guidance materials for covered entities. An example includes the March 25, 2005, Federal Register notice on how to file a complaint (70 Fed. Reg. 15329). OESS also published a series of security papers designed to give covered entities insight into the HIPAA Security Rule and assistance with implementation of the security standards. These publications explained specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

Our objective was to evaluate CMS's oversight and enforcement of covered entities' implementation of the HIPAA Security Rule.

Scope

Our audit focused primarily on determining whether CMS effectively:

- identified and investigated HIPAA Security Rule violations,
- ensured covered entity compliance with the HIPAA Security Rule, and
- imposed civil monetary penalties for violations of the HIPAA Security Rule.

We reviewed CMS's oversight and enforcement activities from October 7, 2003, when it received the delegation of authority and responsibility to interpret, implement, and enforce the nonprivacy HIPAA regulations,¹ through August 24, 2007.

We conducted our fieldwork from July 25, 2007, through August 24, 2007, at CMS headquarters in Baltimore, Maryland.

Our review of CMS's internal controls was limited to the controls in place to provide oversight and enforcement of the HIPAA Security Rule.

¹The authority for administering and enforcing compliance with the HIPAA Privacy Rule has been delegated to the HHS Office of Civil Rights (OCR) (65 Fed. Reg. 82381 (Dec. 28, 2000)). The authority for administering and enforcing compliance with the nonprivacy HIPAA rules has been delegated to CMS (68 Fed. Reg. 60694 (Oct. 23, 2003)).

Methodology

To accomplish our objective, we:

- reviewed applicable Federal requirements,
- reviewed CMS's policies and procedures for identifying and investigating alleged HIPAA Security Rule provision violations,
- reviewed the HIPAA Security Rule guidance CMS made available to covered entities,
- reviewed OESS's organizational charts,
- interviewed OESS and OCR officials to determine how complaints with security and privacy elements were coordinated,
- interviewed CMS Office of the General Counsel officials to determine the CMS process for assessing civil monetary penalties, and
- tested for completeness OESS's complaint-processing methodology and documentation using selected complaints from OESS's Administrative Simplification Enforcement Tool.

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 objective.

FINDINGS AND RECOMMENDATION

CMS had taken limited actions to ensure that covered entities adequately implement the HIPAA Security Rule. These actions had not provided effective oversight or encouraged enforcement of the HIPAA Security Rule by covered entities. Although authorized to do so by Federal regulations as of February 16, 2006, CMS had not conducted any HIPAA Security Rule compliance reviews of covered entities. To fulfill its oversight responsibilities, CMS relied on complaints to identify any noncompliant entities that it might investigate. As a result, CMS had no effective mechanism to ensure that covered entities were complying with the HIPAA Security Rule or that ePHI was being adequately protected.

Although reliance on complaints alone was ineffective for identifying noncompliant covered entities, we noted that CMS had an effective process for receiving, categorizing, tracking, and resolving complaints. CMS had developed and implemented detailed procedures for receiving complaints, communicating with filed-against entities, coordinating with OCR for complaints about potential violations of both the HIPAA Security and Privacy Rules, developing corrective action plans, and remediating complaints.

Our ongoing audits of various hospitals nationwide indicate that CMS needs to become proactive in overseeing and enforcing implementation of the HIPAA Security Rule by focusing on compliance reviews. Preliminary results of these audits show numerous, significant vulnerabilities in the systems and controls intended to protect ePHI at covered entities. These

vulnerabilities place the confidentiality and integrity of ePHI at high risk. During our audit, CMS began taking steps to conduct compliance reviews. After we completed our fieldwork but before we issued our report, CMS executed a contract to conduct compliance reviews at covered entities.

FEDERAL AUTHORITIES RELATING TO ENFORCEMENT OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 SECURITY RULE

Congress enacted sections 261 and 262 of HIPAA to establish national standards for protecting the confidentiality and integrity of ePHI and for addressing all aspects of the security of ePHI while it is being stored or transmitted between entities. The standards were implemented in regulations in 45 CFR, parts 160, 162, and 164. The regulations relating to the general administration (such as compliance reviews and civil money penalties) of the HIPAA Security Rule are found in part 160; the applicable standards and implementation specifications for ePHI are found in subpart C of part 164.

HHS delegated the authority and responsibility to CMS:

- to interpret, implement, and enforce the nonprivacy HIPAA regulations;
- to impose civil monetary penalties, including settlements, under section 1176 of the Act for a covered entity's failure to comply with certain requirements and standards;
- to investigate complaints of noncompliance with the HIPAA Security Rule and to make decisions regarding the interpretation, implementation, and enforcement of it; and
- to conduct compliance reviews to determine whether covered entities are complying with the applicable administrative simplification provisions (68 Fed. Reg. 60694 (Oct. 23, 2003)).

The Final Rule for the enforcement section of the HIPAA Administrative Simplification amended 45 CFR subtitle A, subchapter C, parts 160 and 164, and was effective as of March 16, 2006. The Final Rule added subpart E to part 160, including section 160.402(a) relating to civil money penalties:

Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity if the Secretary determines that the covered entity has violated an administrative simplification provision. [See 45 CFR § 402(a). See also 71 Fed. Reg. 8427 (Feb. 16, 2006).]

The final rule also revised section 160.300 by eliminating the words “and the applicable standards, requirements, and implementation specification of subpart E of part 164 [HIPAA Privacy Rule] of this subchapter” and substituted the words “and parts 162 and 164 of this subchapter.” This change made subpart C, “Compliance and Investigations,” applicable to all the HIPAA implementing rules, including the HIPAA Security Rule. Before this revision, regulations for conducting compliance reviews of the HIPAA Privacy Rule’s standards applied

only to OCR. As a result of the revision, the same regulations now allow CMS to conduct compliance reviews of the HIPAA Security Rule's standards.

LIMITED ACTION TO ENSURE COMPLIANCE

From 2003 through the time of this audit, CMS had taken limited action to ensure that covered entities complied with the HIPAA Security Rule. For the most part, these actions consisted of following up on complaints it received. As of August 24, 2007, CMS had not conducted any compliance reviews of covered entities to determine whether the HIPAA Security Rule was being properly implemented.

COMPLIANCE REVIEW PROCEDURES NOT ESTABLISHED

CMS has had the authority and responsibility to interpret, implement, and enforce HIPAA regulations since 2003. The February 16, 2006, Federal Register published implementing regulations giving CMS a mechanism to conduct compliance reviews. However, as of August 24, 2007, CMS had not established any policies or procedures for conducting compliance reviews at covered entities. CMS officials explained that they were not conducting HIPAA Security Rule compliance reviews because they relied solely on complaints to promote voluntary compliance. This approach has met with limited success because CMS has received very few complaints regarding potential HIPAA Security Rule violations.²

ELECTRONIC PROTECTED HEALTH INFORMATION AT RISK

As of August 24, 2007, CMS had not implemented proactive compliance reviews and therefore had no effective way to determine whether covered entities were complying with HIPAA Security Rule provisions. Nor did CMS know how vulnerable ePHI was to attack by individuals intent on accessing and misusing protected health information.

As part of our audit of CMS, we audited the HIPAA Security Rule implementation at one hospital and found significant vulnerabilities in the hospital's systems and controls intended to protect ePHI. In addition, we began audits at seven other hospitals around the country. The preliminary results have also identified significant vulnerabilities with the hospitals' implementation of the administrative, technical, and physical safeguard provisions of the HIPAA Security Rule. These vulnerabilities place the confidentiality and integrity of ePHI at risk and would not generally be included in complaints.

RECOMMENDATION

We recommend that CMS establish policies and procedures for conducting HIPAA Security Rule compliance reviews of covered entities.

²“As of October 31, 2005, OCR had received and initiated review of over 16,000 complaints and had closed 68 percent of the complaints; at the same time, CMS had received and initiated review of 413 complaints and closed 67 percent of the complaints” (71 Fed. Reg. 8424 (Feb. 16, 2006)).

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

CMS did not agree with our findings because it believes that its complaint-driven enforcement process has furthered the goal of voluntary compliance. CMS agreed, however, that compliance reviews are a useful enforcement tool as part of a more comprehensive enforcement strategy that also includes complaint investigation and resolution, outreach, education, and working closely with industry to identify and correct security issues.

CMS agreed with our recommendation to establish specific policies and procedures for conducting compliance reviews of covered entities but emphasized that compliance reviews are just one of several tools that can be used to promote compliance as part of a comprehensive enforcement strategy.

CMS's comments are included in their entirety in the Appendix.

OFFICE OF INSPECTOR GENERAL RESPONSE

Although CMS's complaint-driven enforcement process has furthered the goal of voluntary compliance, the significant vulnerabilities we identified at hospitals throughout the country would not generally have been identified in HIPAA Security Rule complaints. In fact, as of October 31, 2005, CMS received only 413 potential Security Rule complaints out of more than 16,000 total HIPAA complaints HHS received. Adding compliance reviews of covered entities to its oversight process will enhance CMS's ability to determine whether the HIPAA Security Rule is being properly implemented.

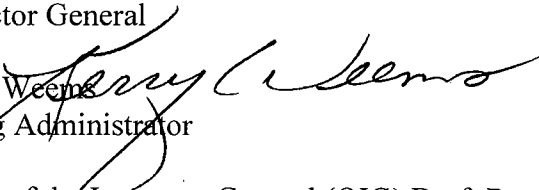
APPENDIX

*Office of the Administrator*

Washington, DC 20201

DATE: JUN 30 2008

TO: Daniel R. Levinson
Inspector General

FROM: Kerry Weems 
Acting Administrator

SUBJECT: Office of the Inspector General (OIG) Draft Report: "Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight" (A-04-07-05064)

Thank you for the opportunity to review and comment on the above OIG Draft Report. The OIG report is based on an audit conducted in August of 2007 to evaluate the effectiveness of the Centers for Medicare & Medicaid Services' (CMS) oversight and enforcement of covered entities' implementation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The draft report stated that CMS' security enforcement actions have been limited and have not provided effective oversight or encouraged compliance of the Security Rule by covered entities. CMS does not agree with the OIG's finding, as our experience over the past three years illustrates the effectiveness of our enforcement approach. We believe that our complaint-driven enforcement process has furthered the goal of voluntary compliance in accordance with the principles set out in the HIPAA Enforcement Rule at 45 C.F.R. 160.304.

As of April 21, 2005, CMS has received and processed more than 300 security complaints from individuals and organizations across the country. These complaints are widespread and diverse, not only geographically, but also with respect to the type of entity complained against. Complaints have been filed against all sizes and types of covered entities including solo practitioners, hospitals, pharmacy chains and health plans. In addition, the complaints implicate a range of Security Rule issues, from inappropriate access controls for systems containing electronic protected health information to a lack of policies and procedures governing device and media disposal.

When CMS has communicated with covered entities against which a complaint has been filed, they have made appropriate and expedient efforts to comply and to mitigate each situation. Thus far, CMS' investigations of complaints show that few if any of the violations have been the result of intentional non-compliance or malicious intent. We further note that CMS and the Office for Civil Rights (OCR), in conjunction with the Office of General Counsel, have both adopted this complaint based, voluntary compliance enforcement approach for complaint allegations that implicate both the Privacy and Security Rule. Complaints that appear to involve both rules are

handled cooperatively between CMS and OCR, and if an onsite evaluation is deemed appropriate, the two agencies coordinate that activity.

In summary, while we differ with the OIG's findings that CMS' approach to enforcement of the Security Rule is inadequate, we do agree that compliance reviews are a useful enforcement tool as part of a more comprehensive enforcement strategy that also includes complaint investigation and resolution, outreach, education, and working closely with industry to identify and correct security issues.

We address the report's Recommendation/Suggestions below.

OIG Recommendation

The OIG recommends that CMS establish policies and procedures for conducting compliance reviews of covered entities.

CMS Response

The OIG equates the effectiveness of CMS' enforcement activities with the presence or absence of a compliance review program. We agree that compliance reviews are part of a comprehensive enforcement strategy, but also feel that they are but one of several tools that can be used to promote compliance. OIG's singular focus on compliance reviews neglects the value that other methods, such as complaint investigation and resolution, increased outreach to industry, and education, have demonstrated in improving compliance.

Nonetheless, CMS does not disagree with the OIG recommendation for the establishment of a specific policy and accompanying procedures for conducting compliance reviews of covered entities against which a complaint has been filed or entities that have been deemed appropriate for review by other means. At the time of the audit, CMS was already developing a Statement of Work to secure professional services to conduct compliance reviews, as authorized by the Enforcement Rule. A contract was executed with PriceWaterhouseCoopers in 2007, which includes onsite reviews of certain covered entities. The onsite review not only assesses the entity's compliance with the facts of the allegations, but includes a more comprehensive assessment of the entity's overall security practices, risk assessment, policies and procedures and the like. A list of potential policies, procedures and documents that could be included in these reviews was posted to the CMS Website in late 2007. This initiative complements the existing complaint management process at CMS, and was an appropriate step towards expanding the enforcement tactics to monitor compliance with the Rule. CMS and OIG are currently considering an arrangement to collaborate on future compliance reviews and enforcement efforts for fiscal year 2009 to capitalize on the review strengths of the OIG, and the HIPAA security expertise of CMS.

As mentioned above, CMS feels that outreach and education are also critical parts of an effective enforcement strategy and we have now begun targeting issues that have been identified during the complaint and review processes. We believe that the combination of enforcement and education is an appropriate approach that will effectively reach the industry on a broader scale,

and also furnish, as appropriate, technical assistance to covered entities to help them achieve compliance. In 2008, CMS began to post case studies based on complaint data on to the CMS Website. The purpose is to enable the industry to benefit from the issues identified from an individual case or compliance review. Other educational tools and activities already in place include Frequently Asked Questions, guidance documents, and educational papers, as well as CMS participation at industry conferences. These resources heighten the industry's understanding of HIPAA security requirements and the various means by which entities can comply.

Again, we appreciate the opportunity to review and comment on this draft report.