



White Paper



The 2012 HIPAA Audits: Will the Past Predict the Future? Understanding Leads to Best Preparation

Bob Chaput
Clearwater Compliance LLC
www.ClearwaterCompliance.com
(800) 704-3394

in conjunction with
Paloma A. Capanna
Attorney & Policy Analyst

The 2012 HIPAA Audits: Will the Past Predict the Future? Understanding Leads to Best Preparation

Copyright Notice. All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

For reprint permission and information, please direct your inquiry to bob.chaput@clearwatercompliance.com

Disclaimer

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Clearwater Compliance LLC. The listing of an organization does not imply any sort of endorsement and Clearwater Compliance LLC takes no responsibility for the publications of third parties.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

The writers of this paper will review and possibly update their analysis should any significant data changes occur.

This document is for Education and Awareness Use Only.

Contents

Introduction.....	4
About The Authors	4
Overview.....	5
I. History of Agency Audit Activities of the HIPAA Privacy Rule and Security Rule.....	6
II. KPMG Contract Synopsis: What Do We Know? and What Do We Know We Don't Know?.....	11
A. Basic Information and Questions.....	12
B. Macro Audit Steps.....	12
C. Audit Results.....	14
D. Fines Collected Become Part of HHS Enforcement Budget.	14
III. CMS and HHS-OIG 2007-2010 Audits – What Can Be Said?.....	14
A. 2007-2010 Selection Criteria?	15
B. 2007-2010 Purpose and Scope?	17
C. 2007-2010 On Beyond Black Letter Law?	18
Conclusion.....	20
Recommended Immediate Actions for Consideration.....	21
Appendix A: Chronology of Available Review, Audit, Settlement Agreement, and Final Determination Data from CMS, OCR, and HHS-OIG.....	22
About Clearwater Compliance	23

Introduction

This White Paper is the first in a series addressing the increasingly complex business risk management issue of HIPAA-HITECH compliance. Several topics have already been identified and research work is underway. Clearwater uses a multidisciplinary approach to researching and writing these papers to consider what HIPAA and HITECH privacy, security and breach notification regulations mean to the healthcare industry, patients and the future of healthcare delivery. Clearwater conducts ongoing research, offers frequent educational live web events, resources and breaking news updates on topics related to HIPAA, the HITECH Act, and the HIPAA Privacy and Security Rules. This work influences product development for clients as Clearwater strives to be the leader in consulting services and software products for HIPAA compliance in the healthcare industry.

About The Authors

Bob Chaput, President – Clearwater Compliance LLC

Mr. Chaput is president of Clearwater Compliance LLC. Clearwater Compliance helps Covered Entities and Business Associates meet stringent HIPAA-HITECH Privacy and Security Rule requirements and address one of five health outcomes policy priorities in the Meaningful Use Stage 1 guidelines dealing with privacy and security. Having served on operational and technology assignments in large healthcare enterprises, Mr. Chaput is no stranger to protecting large amounts of healthcare data – his experience includes responsibility for protecting some of the world’s largest healthcare databases, requiring the highest levels of security and privacy while a senior executive at GE, Johnson & Johnson and Healthways, Inc. Over the years he has also built, grown and sold a number of businesses serving industries with strict regulatory requirements, with deep experience in HIPAA and HITECH rules. He speaks and writes extensively on HIPAA and HITECH security matters and is a recognized HIPAA-HITECH compliance expert.

Paloma A. Capanna, Attorney & Policy Analyst

Ms. Capanna is an Attorney and Policy Analyst. She is an Attorney in private practice with more than 20-years of experience, and an Adjunct Professor of Political Science at Rochester Institute of Technology. Ms. Capanna brings understanding to the black letter words of the law as living entities that reflect the philosophy and agenda of the federal government from one administration to the next, all within the context of our American democracy and the United States Constitution.

Overview

In 2012, the Department of Health and Human Services, Office of Civil Rights (“OCR”) will undertake audits of 150 covered entities for their compliance with the Health Insurance Portability and Accountability Act (“HIPAA”). This represents a significant change in the federal government’s approach to audits as a vehicle for achieving compliance with, in particular, the HIPAA Security Rule.

Limited, available data from agency audit activities from 2007 to 2010 may be an unreliable indicator of how the 2012 audits will be conducted. Any prior audits conducted by OCR, Centers for Medicare & Medicaid (“CMS”), or the Department of Health & Human Services Office of the Inspector General (“HHS-OIG”) have not provided the type of raw data or case profile reports that would allow a strategic analysis.

The lack of systematic agency audit activities from 2003-2011 means that the 2012 audits could be consistent with prior audits, represent a new approach, or be a hybrid of old plus new.

There is one limited, but clear, indicator of the nature and scope of the 2012 audits in the form of a contract synopsis. In 2011, HHS awarded a contract to KPMG related to development of a \$9.2M audit program to be conducted of 150 covered entities in 2012. Certain, desired elements of the 2012 audits were also itemized in the contract synopsis.

This White Paper reviews agency audit and other enforcement activities from 2003 to 2011, identifies what is known about the 2012 audits, and extracts some insights from the historic agency audit and enforcement activities. This White Paper also offers commentary on best practices for covered entities heading into the 2012 audits and recommends several practical, tangible actions that organizations can take to prepare for the audits in order to become and remain compliant.

As it relates to this initial set of 150 audits, the question arises as to whether the audit scope and protocols will be designed to include an assessment of compliance with the Breach Notification for Unsecured Protected Health Information; Interim Final Rule(IFR)¹. Experts, including the Clearwater Compliance HIPAA HITECH Blue Ribbon Panel^{TM2}, have debated whether the IFR will be included. While persuasive arguments are made on both sides of the argument, we have chosen to limit the scope of our research and analysis in this White Paper to audits related to the HIPAA Privacy and Security Rules.

¹ <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

² <http://abouthipaa.com/blue-ribbon-hipaa-hitech-panel/>

I. History of Agency Audit Activities of the HIPAA Privacy Rule and Security Rule.

On August 21, 1996, Congress enacted the Health Insurance Portability and Accountability Act (“HIPAA”), Pub.L. 104-191, which included national standards that were incorporated into the Social Security Act on the confidentiality, integrity, and availability of protected health information (“PHI”) and, through subsequent amendments, electronic protected health information (“ePHI”).

When Congress did not take action by August 21, 1999, authority transferred to the Department of Health & Human Services (“HHS”) to design incentive programs to inspire the health care industry to shift towards electronic transactions and the safeguards to protect patient health information. Through a series of promulgated rules, comment periods, final rules, and amended final rules, HHS created two groupings of regulations that came to be known as “the Privacy Rule” and “the Security Rule.”

The Privacy Rule is found at 45 CFR Part 160 and Part 164(A) and (E). It was issued December 28, 2000 and came into final form August 14, 2002.³ The Privacy Rule’s full title is “Privacy of Individually Identifiable Health Information.”

The Security Rule is found at 45 CFR Part 160 and Part 164(A), (C), and (E). It came into final form February 20, 2003.⁴ Its full title is “Security Standards for the Protection of Electronic Protected Health Information.”

The Privacy Rule is summarized by HHS, as follows:

“The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.”⁵

As provided by HHS to describe the Security Rule:

“The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created,

³ 65 Federal Register 82462, as amended 67 Federal Register 53182.

⁴ 68 Federal Register 8334.

⁵ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html>

received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.”⁶ (emphasis added)

The Security Rule can be characterized as one component of the broader HIPAA Privacy Rule, specifically as relates to “electronic Patient Health Information” (ePHI).

Since December 20, 2000, interpretation, implementation, and enforcement of the Privacy Rule have been continuously assigned by HHS to its agency, the Office of Civil Rights (“HHS-OCR”).⁷

However, on October 7, 2003, the Department of Health & Humans Services split HIPAA responsibilities between OCR and the Centers for Medicare & Medicaid Services (“CMS”), giving CMS the authority to interpret, implement, and enforce the Security Rule⁸ with goals for covered entities (CEs) as follows:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and,
4. Ensure compliance with this subpart by its workforce.⁹

In 2004-2005, CMS, together with its sub-part, the Office of E-Health Standards and Services (“OESS”), published a series of papers about the Security Rule, known by the title of its first paper, “Security 101.”¹⁰ The Security 101 Series of seven papers provided fundamental guidance to covered entities on statutory requirements, recommendations for compliance, and examples of inadequate policies, procedures, technology, and safeguards.

Three additional papers were later added to this library, namely the “HIPAA Security Guidance” paper on laptops and portable devices released by CMS in 2006¹¹, the “Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements”

⁶ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html>

⁷ 65 Federal Register 82381 (December 28, 2000).

⁸ 68 Federal Register 60694-60695 (October 23, 2003).

⁹ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf>

¹⁰ “HIPAA Security Series: Security 101 for Covered Entities” (11/2004, rev. 3/2007).

¹¹ “HIPAA Security Guidance,” Department of Health & Human Services (dated 12/28/2006).

released in April 2009¹² and the “Guidance on Risk Analysis Requirements under the HIPAA Security Rule” paper released by OCR in 2010.¹³

Not to be left out, a third HHS agency, the Office of the Inspector General inserted itself into HIPAA compliance when it included a HIPAA project in its FY2007 “Work Plan” under “Health Information Technology in Medicare and Medicaid – Privacy and Security Issues,” stating:

“We will review the experience with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) administrative simplification privacy and security implementation in Medicare and Medicaid to identify key issues that may be relevant to the Department’s health information technology (IT) initiative.”¹⁴

The latest arguable implementation date for HIPAA Security Rule compliance was for the category of “small entities” and the date was April 20, 2006.¹⁵ On that date, the entire class of organizations defined as CEs came under the jurisdiction of CMS for enforcement activities. Considering when the FY 2007 Work Plan must have been drafted, it appears that, from the outset, HHS-OIG was after CMS to pursue enforcement relative to the Security Rule in the form of audits. No similar project was announced concerning an HHS audit of OCR Privacy Rule enforcement activities.

Due to the restricted content of what OIG has released into the public record concerning its 2007 (*et seq.*) audit activities, it reasonably appears, but is not conclusive, that from March-June 2007 HHS-OIG conducted one hospital audit of Piedmont Hospital (Atlanta, Georgia), which would mean that HHS-OIG conducted its audit of Piedmont Hospital before HHS-OIG began its audit of CMS. At the time of the HHS-OIG audit, Piedmont Healthcare was a “multi-facility healthcare system” with two data centers and more than 8,000 employees¹⁶.

By October 2008, HHS-OIG concluded that “...as of August 24, 2007, CMS had not established any policies or procedures for conducting compliance reviews at covered entities.”¹⁷ The 2008 report was the first of two HHS-OIG audit reports on CMS Security Rule enforcement, the second report being issued in 2011.

Although HHS-OIG had apparently finished its audit of Piedmont Hospital prior to publication of its 2008 report, it merely indicated:

“Our ongoing audits of various hospitals nationwide indicate that CMS needs to become proactive in overseeing and enforcing implementation

¹² <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>

¹³ “Guidance on Risk Analysis Requirements under the HIPAA Security Rule,” Department of Health & Human Services, Office for Civil Rights (posted July 14, 2010).

¹⁴ “Work Plan FY2007,” Department of Health and Human Services, Office of the Inspector General, at page 58.

¹⁵ 45 CFR §164.318(a)(2).

¹⁶ www.ehcca.com/presentations/HIPAA16/koster_1.ppt

¹⁷ “Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996: Oversight,” Department of Health & Human Services, Office of the Inspector General (release date October 2008), publication A-04-07-05064, page 5.

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.”¹⁸

From 2007-2010, HHS-OIG conducted a total of seven hospital audits, including Piedmont Hospital. The HHS-OIG hospital audit reports are not in the public domain. In a footnote to “Appendix A” of the 2011 HHS-OIG report, it was explained “We included only the State name, not the individual hospital names or the report numbers, because the reports contained restricted, sensitive information that may be exempt from release under the Freedom of Information Act, 5 U.S.C. s.552. The hospital reports were not posted on the Internet.”¹⁹

Whether as a result of the 2008 HHS-OIG report or otherwise, in 2008, CMS contracted PriceWaterhouseCoopers in a 1-year, \$898,000 agreement for on-site reviews of 10-20 organizations.²⁰ The audits targeted covered entities against which CMS had already received a complaint.²¹ In an August 2008 CMS conference presentation, it was noted “Reviews place emphasis on remote use and access issues.”²²

Lorraine Doo, now Acting Deputy Director of OESS, noted that, in 2008, CMS had only 3 full-time employees for HIPAA security enforcement and Price Waterhouse Coopers had 5 staffers working on the contract reviews.²³

CMS conducted its first audit at Providence Health & Services (Portland, Oregon), which resulted on July 15, 2008 in the first published “Resolution Agreement” with “Corrective Action Plan” between the federal government and a covered entity for loss of ePHI from backup tapes, optical disks, and laptops on five occasions between September 2005 and March 2006.²⁴ Data breaches at Providence affected more than 380,000 patients, and resulted in multiple filed complaints.²⁵ Providence Health & Services, *inter alia*, operates 27 hospitals in five states, and has 40,000 electronic endpoints and 5,000 servers.²⁶

Based upon the two, known CMS audit reports in the public domain, it appears that CMS audited fifteen covered entities; ten reflected in its 2008 “HIPAA Compliance Review Analysis and Summary

¹⁸ *Id.*, p. 3.

¹⁹ “Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996: Oversight,” Department of Health & Human Services, Office of the Inspector General (release date May 2011), publication A-04-08-05069, Appendix A.

²⁰ “HIPAA Security Overview,” Centers for Medicare & Medicaid Services, presented at Health Care Conference Administrators’ Privacy Symposium (August 2008), slide 12.

²¹ “Lock It or Lose It,” Harris Meyer, Hospitals & Health Networks Digital Magazine (September 2008).

²² http://www.ehcca.com/presentations/HIPAA16/phillips_1_2.pdf, slide 12.

²³ http://www.hhnmag.com/hhnmag_app/jsp/articledisplay.jsp?dcrpath=HHNMAG/Article/data/09SEP2008/0809HHN_FE_A_HIPPA&domain=HHNMAG

²⁴ Resolution Agreement between the United States Department of Health and Human Services, Office for Civil Rights and Providence Health & Services (fully executed July 15, 2008), p. 1.

²⁵ <http://www.slideshare.net/SOURCEConference/keynote-8331186>, “I Volunteered to Do This?” by Eric Cowperthwaite, Providence Health & Services, June 16, 2011, slide 3.

²⁶ *Id.*, slide 2.

of Results” and five compiled into its 2009 report.²⁷ These audit reports are aggregated with non-identifying narratives, which place a primary emphasis upon education.

Regardless of CMS’s initial audit efforts, on July 27, 2009, the Secretary of HHS shifted responsibility for the Security Rule from CMS to the OCR, including:

- (1) the authority and responsibility to interpret, implement, and enforce the Security Rule;
- (2) the authority to conduct compliance reviews and to investigate and resolve complaints of Security Rule noncompliance; and,
- (3) the authority to impose civil monetary penalties for a covered entity’s non-compliance with the Security Rule.²⁸

The transfer of authority was “effective immediately.”²⁹

It was not until the FY2009 Work Plan that HHS-OIG expressly stated its intention to “review various HIPAA-covered Medicare program providers’ compliance with the HIPAA Privacy Rule requirements,”³⁰ even though HHS-OIG hospital audits began on site in early 2008.³¹ HHS-OIG included projects for CMS’s Security Rule oversight in its FY2007³², FY2008³³, FY2009³⁴, and FY2010³⁵ work plan.

The 2011 HHS-OIG report confirmed its earlier findings that “CMS’s oversight and enforcement actions were not sufficient to ensure that covered entities, such as hospitals, effectively implemented the Security Rule.”³⁶ HHS-OIG’s point was largely moot as Security Rule enforcement had already transferred from CMS to OCR effective July 27, 2009. But, what the 2011 HHS-OIG report brought forward was the aggregation of HHS-OIG audits of seven hospitals between early 2007 and March 15, 2010.³⁷ Appendix B to the report, in part, also provided individual, though non-identifying, examples of non-compliant acts, errors, and omissions at audited CEs.

The HHS-OIG 2011 report perpetuated its silence about OCR enforcement of the Security Rule or the Privacy Rule.

²⁷ “HIPAA Compliance Review Analysis and Summary of Results – Reviews 2008” by the Centers for Medicare & Medicaid Services and Office of E-Health Standards and Services, no date of issue; and, “2009 HIPAA Compliance Review Analysis and Summary of Results” by the Centers for Medicare & Medicaid Services and Office of E-Health Standards and Services” (issued September 22, 2009).

²⁸ 74 Federal Register 38630 (August 4, 2009).

²⁹ *Id.*

³⁰ “Work Plan FY2009,” Department of Health and Human Services, Office of the Inspector General, page 81.

³¹ “What Boards Need to Know About Regulatory Issues,” Trustee Magazine (October 2008).

³² 2007 HHS-OIG Work Plan, *supra*.

³³ “Work Plan FY2008,” Department of Health and Human Services, Office of the Inspector General, page 56.

³⁴ 2009 HHS-OIG Work Plan, *supra*

³⁵ “Work Plan FY2010,” Department of Health and Human Services, Office of the Inspector General, page 81.

³⁶ 2011 HHS-OIG report, p. 4.

³⁷ 2011 HHS-OIG report, *id.*, Appendix A and pages 2, 3.

On February 22, 2011, OCR entered its first civil money penalty to enforce the Privacy Rule against Cignet Health (Maryland), fining Cignet \$4.3 million through a “Notice of Final Determination.”³⁸ The essential violation was a repeated failure to provide individuals access to their health records, a Privacy Rule violation. The fine broke down as \$1.3 million for the HIPAA Privacy Rule violation and \$3 million for “willful neglect” in its responsibility to respond to repeated OCR requests for information and compliance. This was the first fine issued through a “Notice of Final Determination”; all prior fines by CMS or OCR had been reached through “Resolution Agreements” with or without a companion “Corrective Action Plan,” these being settlement-oriented vehicles without admission of fault.

Just two days later, on February 24, 2011, OCR announced a \$1 million Resolution Agreement with Massachusetts General Hospital, including a 3-year Corrective Action Plan.³⁹

HHS entered into a \$9.2M contract with KPMG for a protocol and audit performance program to “...assist OCR in operating an audit program that effectively implements the statutory requirement to audit covered entity and business associate compliance with the HIPAA privacy and security standards as amended by the American Recovery and Reinvestment Act of 2009 (ARRA).”^{40, 41}

And, most recently, on July 6, 2011, OCR announced a Resolution Agreement and Corrective Action Plan with the University of California at Los Angeles Health System, including a fine of \$865,500.⁴²

The 2011 activities of OCR and HHS-OIG evidence a seriousness about HIPAA enforcement that will likely spill over into the 2012 audits.

II. KPMG Contract Synopsis: What Do We Know? and What Do We Know We Don't Know?

The impending 2012 audits were mandated in a single sentence under Section 13411 - “Audits” as part of the ARRA, Pub.L. 111-5, Division A, Title XIII, Subdivision D – “Privacy”: “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.”

³⁸ “Notice of Final Determination,” Department of Health & Human Services, Office for Civil Rights (dated February 4, 2011) and “Notice of Proposed Determination,” Department of Health & Human Services, Office for Civil Rights (dated October 20, 2010).

³⁹ “Resolution Agreement” between the Department of Health and Human Services and Massachusetts General Hospital (fully executed February 14, 2011).

⁴⁰ “OCR HIPAA Audit Protocol and Program Performance – Solicitation Number OS57605”; contractor awarded name KPMG, contract award date June 10, 2011, contract award number GS23F8127H-HHSP233201100252G.

⁴¹ Please note that for purposes of this White Paper, the phrase “covered entity” (designated “CE”) should also be read to apply to “business associates” (commonly designated as “BA”).

⁴² “Resolution Agreement” between the Department of Health and Human Services, Office for Civil Rights and University of California, *et al.* (fully executed July 6, 2011) with “Corrective Action Plan.”

A. Basic Information and Questions.

The KPMG Contract Synopsis (award date June 10, 2011, hereafter “Synopsis”) offers some clear insight into the 2012 audits.⁴³ Valued at \$9.2M, the Synopsis indicates there are to be 150 audits of CEs in 2012.

There is no indication in the Synopsis how CEs will be selected for the audits. However, HHS awarded a contract to Booz Allen Hamilton on June 9, 2011, for \$180,000, for “audit candidate identification.”⁴⁴ Limited public information is available about this contract.⁴⁵

B. Macro Audit Steps.

Step One: Site Visits. As per the Synopsis, the essential steps of each 2012 audit will include:

- site visits as part of every audit, including
 - personal interviews with CE “leadership,” specified as “e.g., CIO, Privacy Officer, legal counsel, health information management/medical records director;”
 - a hands-on examination of the physical features and operations of the CE;”
 - an examination of “consistency of process to policy;” and,
 - an observation of compliance with regulatory requirements.

Leadership. It is clear, even from the Synopsis, that CEs must have a designated individual assigned to lead the CE’s HIPAA compliance efforts. This is consistent with explicit requirements in both the Privacy Rule⁴⁶ and the Security Rule.⁴⁷

Notification. In terms of notification, there is some indication that, at least as to HHS-OIG’s audit of Piedmont, a data request letter with a ten-day response window was issued as the first step in the audit.⁴⁸ Such an approach would also be consistent with the OCR “Case Processing Manual.”⁴⁹

Documentation. These macro audit steps listed above, particularly the on-site visit and personnel interviews, appear consistent with the approaches taken by CMS, OCR, and HHS-OIG to date, whether in the four reports, the public Resolution Agreements, or the media and conference data offered by personnel at audited CEs. In light of this, CEs would be well advised to prepare to

⁴³ 2011 KPMG contract, *supra*.

⁴⁴ FedBizOpps.gov Solicitation Number: OS55726

⁴⁵ “And the New HIPAA Cop Is ... HHS Appoints Contractor to Conduct HIPAA Privacy and Security Audits” by Adam Green <http://www.dwt.com/LearningCenter/Advisories?find=424919>

⁴⁶ 45 CFR §164.530(a)(1).

⁴⁷ 45 CFR §164.308(a)(2).

⁴⁸ “HIPAA audit: The 42 questions HHS might ask,” Computerworld, by Jaikumar Vijayan (June 19, 2007).

⁴⁹ Department of Health and Human Services, Office of Civil Rights, “Case Resolution Manual for Civil Rights Investigations (revised 2009)”, page 49.

demonstrate each and every policy, procedure, and document relating to the implementation of the technical, physical, and administrative requirements of HIPAA.

Step Two: Auditor Reports. Also, as per the Synopsis, each auditor is to submit an audit report after each site visit, including at least the following:

- the name, address, EIN, and contact person for the CE; and,
- “methods used to conduct the audit.”

There was language in the CMS reports that suggested the audits were tailored to the specific CE.⁵⁰ While HIPAA reflects scalability concepts, it would not seem reasonable to send auditors on-site to a CE without audit criteria in hand. The Synopsis language here is likely ambiguous drafting, rather than an indication that auditors will have broad discretion.

And, as per the Synopsis, to be included to support each finding will be:

- ▲ “Condition: the defect or noncompliant status observed, and evidence of each;”
- ▲ “Criteria: a clear demonstration that each negative finding is a potential violation of the Privacy or Security Rules, with citation;”
- ▲ “Cause: The reason that the condition exists, along with identification of supporting documentation used;”
- ▲ “Effect: the risk or noncompliant status that results from the finding;”
- ▲ “Recommendations for addressing each finding;”
- ▲ “Entity corrective actions taken, if any;” and,
- ▲ “Acknowledgement of any best practice(s) or success(es).”

Opportunity for Remediation. This list, too, appears reflective of an enforcement technique somewhat unique to CMS, OCR, and OIG – the opportunity for active remediation of an indicated short-coming. CEs would be wise to consider that the ability to respond to an OCR request for remediation likely can only succeed if the CE is substantially HIPAA compliant and has in place the active policies, procedures, practices, and personnel to quickly respond to such a request. CEs would also be wise to note that their ability to rapidly respond to a remediation request could mean a difference of millions of dollars in fines if the CE is characterized by OCR as having exhibited “willful neglect.”

This allowance for active remediation appears to have been the approach by CMS and HHS-OIG to the individual hospitals previously audited. CEs would be well advised not to treat the potential of an OCR audit as a ‘free risk analysis,’ but should operate on the presumption that any audit will result in a finding of non-compliance as to one or more provisions of HIPAA and the CE should seek to minimize that exposure through proactive, good faith compliance efforts and preparedness to be in a position in the event of an audit with remediation request to respond to such a request.

⁵⁰ 2008 CMS report, page 1.

C. Audit Results.

We also do not know when or if the audit results will be made public. The Synopsis does not indicate of how it will handle either the raw data or the findings.

On the one hand, HHS-OIG and CMS have maintained the individual hospital audit data as non-public. But, on the other hand, as concerns several Resolution Agreements, Corrective Action Plans, Final Determinations, and data breaches impacting 500 or more patient records, CMS and OCR have been very public via press releases, postings to websites, and public comments.

From a risk-benefit analysis perspective, CEs should rigorously conduct their HIPAA compliance activities with the knowledge that their audit reports could be published with identifying data and that it will remain an enduring part of the HHS website. OCR has also suggested in interviews, on occasion, that audit findings may result in further enforcement activities.

D. Fines Collected Become Part of HHS Enforcement Budget.

HHS/OCR has been given incentive to conduct the audits with a view to imposing fines in that HHS is already authorized to retain any fines collected to apply to the enforcement process.⁵¹

Considering, also, the difference between the earlier CMS Resolution Agreements and the 2011 OCR Resolution Agreements and considering that penalties were legislatively increased at least once since 2003, CEs would be well advised to understand and weigh the penalty calculations as a realistic potential consequence of HIPAA non-compliance identified during an audit.

III. CMS and HHS-OIG 2007-2010 Audits – What Can Be Said?

The CMS and HHS-OIG 2007-2010 audit data is limited to four reports, specifically:

1. “Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996: Oversight,” Department of Health & Human Services, Office of the Inspector General (release date October 2008), publication A-04-07-05064;
2. “Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996: Oversight,” Department of Health & Human Services, Office of the Inspector General (release date May 2011), publication A-04-08-05069;
3. “2008 HIPAA Compliance Review Analysis and Summary of Results,” Department of Health & Human Services, Centers for Medicare and Medicaid Services and Office of E-Health Standards and Services (release date not provided).

⁵¹ 42 USC §13410(c)(1).

4. 2009 HIPAA Compliance Review Analysis and Summary of Results,” Department of Health & Human Services, Centers for Medicare and Medicaid Services and Office of E-Health Standards and Services (release date September 22, 2009); and,

These four reports are narrative in nature and use aggregated non-identifying information. The two papers produced by HHS-OIG appear to have a primary purpose of criticism of CMS’s enforcement of the Security Rule. The CMS papers seem to have a primary purpose of public education.

There is no evidence in the public domain to suggest that either CMS or OIG employed neutral or statistical methodology to select the target CEs or intended to audit a statistically relevant sample population. Although the HHS-OIG and CMS reports use global terms like “nationwide,”⁵² there is no evidence presented in the reports to suggest that the results of the audits could serve as other than individual case examples or case profiles. Indeed, even OCR commented to HHS-OIG: “As a general comment, we caution against drawing conclusions about the state of compliance of all covered entities based on the small sample of narrowly focused audits performed in the review of CMS oversight.”⁵³

Because of the limitations imposed by HHS-OIG and CMS in their published reports, there is an associated limitation on how reliable the use of that report data could be as a predictor of the 2012 audits.

However, this does not mean that the reports are without value for analysis when viewed as a whole and when viewed in the context of the history of agency audit activity.

The reports are useful information to help CEs prepare for the 2012 audits, as relates to the varied approaches taken to CE selection, agency use of documents outside the Security Rule and the Privacy Rule to set the standards of interpretation of HIPAA, and the priorities placed on certain forms of technology as having a propensity towards high risk vulnerabilities.

A. 2007-2010 Selection Criteria?

CMS Targeted CEs. From 2007-2010, HIPAA Security Rule audit activities by CMS and HHS-OIG can be viewed targeting three types of CEs: (A) filed-against CEs; (B) breach-notified/in-the-media CEs; and, (C) *ad hoc* CEs.

In its 2008 audit report, CMS described the ten hospitals that were subjected to audits as based on: (1) complaints filed against the entities; (2) media coverage; “or” (3) recommendations from OCR.⁵⁴ It was not until the 2009 audit report that CMS explicitly stated that all ten hospitals in its 2008 audit report were “filed against entities” (“FAEs”).⁵⁵

⁵² 2008 HHS-OIG report, *supra*, p. 3.

⁵³ 2011 HHS-OIG report, *supra*, Appendix D, page 1.

⁵⁴ 2008 CMS report, *supra*, p. 1.

⁵⁵ 2009 CMS report, *supra*, p. 1.

By some contrast, the 2009 CMS audit report data set consisted of five hospitals, one which was a FAE and four which were non-FAEs.⁵⁶

PriceWaterhouseCoopers (PWC) played a role in some or all of these 2008 and 2009 audits, but CMS' report neither specifically defines PWC's role nor its contribution to the process.

The category of in-the-media CEs can probably be interpreted as those CEs that were required to make media notifications under the Breach Notification Rule for an impermissible use or disclosure that compromised the security or privacy of protected health information affecting 500 or more individuals.⁵⁷ It reasonably appears from the 2009 CMS audit report that any in-the-media CE was also a FAE, such that in-the-media should not be read as a distinct category of CE.

As to the remark that CEs selected were also ones referred by OCR, this remark was not discussed in the report. Given the procedure as it existed in 2008 - mid-2009, this, too, could simply be another part of the history of the FAE. OCR was then referring Security Rule violations to CMS.

HHS-OIG Targeted CEs. By contrast, the only way the HHS-OIG audits can be characterized is "*ad hoc*," which, for purposes of this White Paper simply means "Who knows?"

HHS-OIG made claim to having audited seven hospitals between 2007-2010, as discussed in their 2011 report. The only identifying data provided in the 2011 HHS-OIG report was the state location of the hospitals as California, Georgia, Illinois, Massachusetts, Missouri, New York, and Texas.⁵⁸ An Appendix to the 2011 HHS-OIG report included the specific date that it completed its individualized report to each of the seven hospitals.⁵⁹

The 2011 report included a footnote that: "An eighth audit was underway in Pennsylvania at the time the report was released."⁶⁰ No known report in the public domain includes discussion of this hospital audit by HHS-OIG.

Unlike the CMS reports, however, the HHS-OIG 2011 report included specific, individual hospital acts, errors, and omissions that HHS-OIG considered to be non-compliant to the Security Rule. Appendix B to the HHS-OIG 2011 report includes more than fifteen specific examples from "one hospital" that HHS-OIG defined as "High-Impact Vulnerabilities" in the technical, physical, and administrative categories. These examples, along with others of varying aggregation, do not indicate whether CEs were FAEs, in-the-media, or identified by and/or with OCR.

Based upon the limited, available data, it appears fair to say that if a CE becomes an FAE with multiple and/or persistent complaints, it could be a sufficient triggering event to result in an audit. If all of the 150 CEs of the 2012 audit are announced at once, this will decrease the relevance of this factor during the 2012 audit period. However, any of the more than 300 CEs which have already been

⁵⁶ 2009 CMS report, *id.*, p. 1.

⁵⁷ Interim final Breach Notification Rule (issued August 2009, 74 Federal Register 42740).

⁵⁸ 2011 HHS-OIG report, *supra*, p. 2.

⁵⁹ 2011 HHS-OIG report, *id.*, Appendix A.

⁶⁰ 2011 HHS-OIG report, *id.*, p. 2, footnote 1.

required to abide by the interim final Breach Notification Rule and/or which have a history of multiple or persistent complaints should not view the incident(s) as a completed event, but should invigorate their HIPAA compliance activities as if the event(s) may be the starting point for an audit.

B. 2007-2010 Purpose and Scope?

It may be that HIPAA has suffered such a fractured route to audits because CMS and HHS-OIG exhibited fundamental differences of purpose for conducting audits. The collision of ideology may have resulted in CMS being stripped of their enforcement responsibility for the Security Rule and OCR securing its authority to enforce both the Privacy and the Security Rules. But, even though this disagreement ended in 2009, it should be consciously examined to understand the ideology that may well influence the design and implementation of the 2012 audits.

CMS – an Agency Emphasis on Education. CMS consistently expressed the position that public education to bring forth complaints would be the basis of enforcement efforts designed to elicit more public education to bring forth more complaints, and so forth. For CMS, education of the public was the path to HIPAA compliance.

This CMS philosophy led to a straight-forward approach to audits, as reflected in the CMS 2008 and 2009 reports, specifically:

1. Risk analysis;
2. Currency and adequacy of policies and procedures;
3. Security awareness and training;
4. Workforce clearance;
5. Workstation security;
6. Encryption; and,
7. Business Associate contracts.

This report structure reflected CMS's hierarchy of priorities, criticisms of practices observed, and recommendations in the style of compliance checklists.

HHS-OIG – an Agency Designed for Criticism. The CMS emphasis on public education was strongly criticized by HHS-OIG in its 2008 and 2011 reports. Indeed, the basic function of HHS-OIG is to ferret out problems such as Medicare fraud, abuse, and neglect at medical providers and to find waste within government spending.

HHS-OIG designed a project to audit CMS's enforcement activities, but then set out on its own audits, stating:

“These audits focused primarily on the hospitals’ implementation of (1) the wireless electronic communications network or security measures the security management staff implemented in its computerized

information systems (technical safeguards); (2) the physical access to electronic information systems and the facilities in which they are housed (physical safeguards); and (3) the policies and procedures developed and implemented for the security measures to protect the confidentiality, integrity, and availability of ePHI (administrative safeguards).”⁶¹

HHS-OIG took an ePHI emphasis into audits of seven hospitals and found more than 150 HIPAA violations it termed “vulnerabilities.”⁶² HHS-OIG in its 2011 report designed its own hierarchy of risk assessment, prioritizing Security Rule provisions and assessing vulnerabilities as “high,” “medium,” or “low”⁶³ - a framework that HHS-OIG adapted from a publication of the National Institute of Standards and Technology special publication (SP) 800-30.⁶⁴

While it is equally true that CMS referenced external publications such as the NIST SP 800-30, it was referenced, along with the CMS Security Series as “risk assessment guidance for CEs to improve their level of compliance with the Security Rule.”⁶⁵

OCR – an Agency Designed for Enforcement. Like HHS-OIG, OCR is charged with a mission of law enforcement, specifically for civil rights and health privacy rights.⁶⁶

Again, if our question is whether the past audits can predict anything about the future audits, it would be reasonable to assume that OCR will bring an enforcement-oriented approach that is more like the HHS-OIG enforcement-driven audit approach than the CMS education-based audit approach.

This resolution of ideological differences in favor of the HHS-OIG enforcement-driven audit style appears the style that will color the 2012 audits. CEs would be well-advised to immediately begin and/or rigorously implement a HIPAA compliance program that can withstand the depth and breadth of the anticipated 2012 audits. CEs would be wise to project that an audit will review all aspects of the Privacy Rule and the Security Rule, and not merely consist of a few, select provisions. One practical way to prepare for this type of audit would be to hire an outside consultant to essentially role play an OCR auditor. Such a step could also be provided by the CE if selected for an OCR audit, as part of the CEs efforts at demonstrating good faith HIPAA compliance efforts.

C. 2007-2010 On Beyond Black Letter Law?

Perhaps the most striking feature of the prior audits that should be considered when preparing for the 2012 audits is that both CMS and HHS-OIG presented their audit reports with analysis that went far beyond the black letter of the Privacy Rule and the Security Rule. Previous agency audits included

⁶¹ 2011 HHS-OIG report, *supra*, page 2.

⁶² *Id.*, page 4.

⁶³ *Id.*, page 3.

⁶⁴ “Risk Management Guide for Information Technology Systems,” National Institute of Standards and Technology, Special Publication 800-30 (July 2002), page 23.

⁶⁵ CMS 2009 report, *supra*, p. 6.

⁶⁶ <http://www.hhs.gov/ocr/office/about/mission-vision.html>

reference to and reliance upon documents outside the black letter of the Rules, treating those documents with as much weight and authority as if the documents were akin to regulations. This agency methodology can be said to be beyond activism and into the highest category of “hypervigilance.”

One example of agency hypervigilance in the interpretation of statutory language is found under the heading “Ineffective Wireless Network Encryption.” HHS-OIG took the black letter, legal language, such as that found in 45 CFR §164.310(e)(1) that says “Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communication network” and infused an uncited recommendation from the Institute of Electrical and Electronics Engineers (IEEE), to go so far as to conclude that a hospital’s use of Cisco’s “Lightweight Extensible Authentication Protocol (LEAP)” was insufficient to secure transmission of data between access points.⁶⁷

In an August 19, 2008 PowerPoint on “Lessons Learned from the Piedmont Healthcare HIPAA Security Audit,” hospital officials included a slide: “Each review will include an analysis of the covered entities (*sic*) remote access policies and procedures, in accordance with CMS Remote Security Guidance Document issued on December 18, 2006. Such analysis will take place regardless of the nature of the complaint.”⁶⁸ This slide is spot on to the approach demonstrated in the HHS-OIG 2011 report, which prioritized ePHI and went beyond the black letter of the HIPAA regulations and into other agency documents.

Whenever one encounters an atmosphere of hypervigilance within the Executive branch, one is best forewarned that it will be difficult to meet every point raised by the government. It tends to mean that responding parties may have a sense of being “guilty until proven innocent.” Also, depending on how many extra-statutory sources OCR draws from to conduct its audits, it may also lead to an impression that, even for those CEs who have made good faith efforts at HIPAA compliance, their efforts were not rewarded with a good review.

The environment of Executive Branch hypervigilance puts CEs in the position of either/both having to dedicate on-going personnel resources into following and understanding the regulatory environment and/or hiring outside consultants to advise on point. The practical challenge presented by this style of Executive Branch enforcement is that it requires development of a parallel library. Reading and even understanding the Privacy Rule and the Security Rule may not be enough to survive an audit, when all indications are that auditors could be utilizing external documents to assess even the technical specifications of equipment selected by ePHI.

⁶⁷ 2011 HHS-OIG report, Appendix B, pages 1-2.

⁶⁸ www.ehcca.com/presentations/HIPAA16/koster_1.ppt at slide 9.

Conclusion.

CEs should not underestimate the impact the 2012 audits could have on the health care industry and, potentially, upon their specific organization. If selected for the first systematic audits, the CE could face a hypervigilant level of scrutiny as OCR engages in a comprehensive review of all provisions of the HIPAA Privacy Rule and Security Rule, potentially extending its audits to levels beyond the black letter of the law.

CEs not otherwise having done so in a timely manner should immediately undertake and sustain an active process to bring their entity into HIPAA compliance and to maintain that position. At the very least, CEs should designate a HIPAA compliance officer, undertake a risk analysis, design and implement policies and procedures to secure and monitor the privacy of patient health information, including a process to identify and respond to data breach, and should create and continuously update a library of policies, procedures, practices, and breach responses.

CEs which believe themselves, in good faith, to be HIPAA compliant should consider a third party audit to test everything from their policies and procedures to their data logs or their individual passwords. Among the selection criteria for such consultants should be their familiarity with all enforcement materials utilized by HHS-OIG, from the actual regulations to publications such as NIST SP 800-33, SP 800-30, SP 800-53, Rev1, etc..

The risk of multi-million dollar fines and public disclosure for HIPAA violations should be viewed as deterrents now actively employed by OCR to achieve HIPAA compliance. These enforcement techniques may well be a prevalent outcome of the 2012 audits as HHS uses HIPAA fines as a means to fund on-going audit and future enforcement activities.

Recommended Immediate Actions for Consideration.

In terms of immediate next actions to consider, Clearwater Compliance encourages all CEs to initiate formal activity to not only prepare for the audits, but, more importantly, to work to become and remain compliant with the HIPAA and HITECH regulations and in so doing, demonstrate good-faith effort should the CE be audited. Compliance with these regulations is complex and there are many possible actions one can take.

The following are five important steps CEs should consider taking immediately:

1. Formally establish and charter a Privacy and Security Risk Management Council and establish a Security Management Process per 45 CFR §164.308(a)(1).
2. Complete an Evaluation per 45 CFR §164.308(a)(8) to assess Security Rule “black letter” compliance and to understand the complete regulation; the Security Rule is the ultimate checklist.
3. Complete a Risk Analysis per 45 CFR §164.308(a)(1)(ii)(A) to assess risk and determine the CE’s security posture and initiate a corrective action plan.
4. Complete an assessment of compliance with the Privacy Rule using per 45 CFR §164.530 Administrative Requirements as a guide.
5. Document and act upon a corrective action plan for Security Rule compliance, Privacy Rule compliance, and overall Risk Management per 45 CFR §164.308(a)(1)(ii)(B).

Appendix A: Chronology of Available Review, Audit, Settlement Agreement, and Final Determination Data from CMS, OCR, and HHS-OIG

Date of Report, Settlement Agreement, or Findings	Government Entity	Covered Entity
2008	CMS/OESS	10 CEs (undisclosed) { 10 FAEs }
7/15/2008	CMS	Providence Health & Services
10/16/2008	HHS-OIG	GA hospital (undisclosed)
2009	CMS/OESS	5 CEs (undisclosed) { 1 FAE }
1/15/2009	CMS	CVS Pharmacies
2/27/2009	HHS-OIG	MI hospital (undisclosed)
9/1/2009	HHS-OIG	NY hospital (undisclosed)
11/10/2009	HHS-OIG	MA hospital (undisclosed)
3/2/2010	HHS-OIG	IL hospital (undisclosed)
3/15/2010	HHS-OIG	TX hospital (undisclosed)
6/7/2010	OCR	RiteAid Pharmacies
12/13/2010	OCR	Management Services Organization
2/4/2011	OCR	CIGNET
2/14/2011	OCR	Massachusetts General Hospital Corporation and Massachusetts General Physicians Organization, Inc.
7/6/2011	OCR	University of California at Los Angeles Health System

About Clearwater Compliance

www.clearwatercompliance.com

Clearwater Compliance helps covered entities, business associates and their subcontractors meet stringent and complex HIPAA-HITECH Privacy, Security and Data Breach Notification requirements. With tools and software, consulting and staffing and risk management solutions, the company serves healthcare organizations (CEs, BAs and Subcontractors) of all sizes.

Clearwater offers frequent webinars on topics related to HIPAA, the HITECH Act, and the HIPAA Security Rule. Please visit www.AboutHIPAA.com to register for a webinar or sign up for the newsletter.

Clearwater Compliance is active in national efforts to safeguard Protected Health Information and is a premium co-sponsor of the American National Standards Institute (ANSI) Protected Health Information (PHI) project.