

I N S I D E T H E M I N D S

Health Care Law Enforcement and Compliance

*Leading Lawyers on Understanding Recent Trends in
Health Care Enforcement, Updating Compliance
Programs, and Developing Client Strategies*



ASPATORE

©2011 Thomson Reuters/Aspatore

All rights reserved. Printed in the United States of America.

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, except as permitted under Sections 107 or 108 of the U.S. Copyright Act, without prior written permission of the publisher. This book is printed on acid free paper.

Material in this book is for educational purposes only. This book is sold with the understanding that neither any of the authors nor the publisher is engaged in rendering legal, accounting, investment, or any other professional service. Neither the publisher nor the authors assume any liability for any errors or omissions or for how this book or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this book. For legal advice or any other, please consult your personal lawyer or the appropriate professional.

The views expressed by the individuals in this book (or the individuals on the cover) do not necessarily reflect the views shared by the companies they are employed by (or the companies mentioned in this book). The employment status and affiliations of authors with the companies referenced are subject to change.

For customer service inquiries, please e-mail West.customer.service@thomson.com.

If you are interested in purchasing the book this chapter was originally included in, please visit www.west.thomson.com.

Medical Privacy Enforcement
and Penalties: HIPAA
Gets Teeth

Lisa J. Acevedo and Jennifer L. Rathburn

Partners

Quarles & Brady LLP



ASPATORE

Introduction

Of all of the different types of data subject to privacy and security laws, health information is the most highly regulated. Organizations that handle health information must comply with an added layer of strict and complex requirements. Health-specific privacy and security laws do not apply only to organizations whose business is health care, such as hospitals and health insurance companies; they also affect companies that provide services to health care providers and insurers. Further, even companies that do not otherwise touch the health care industry can still be affected by health privacy/security laws and regulations if they maintain health-related benefits plans for their employees.

This chapter will address compliance and enforcement issues under the federal medical privacy law commonly referred to as HIPAA. This chapter will conclude with practical guidance on conducting internal investigations.

A Brief History

The US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is ramping up its enforcement efforts—almost a decade after the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted. The following is a brief history of HIPAA and its implementing privacy regulations, 45 CFR §§ 160 and 164, subparts A and E (Privacy Rule) and security regulations, 45 CFR §§ 160 and 164, subparts A and C (Security Rule), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, PL 111-5, 42 USC 17921 (HITECH or HITECH Act). It is important to note that HHS has ultimate authority over the HIPAA Privacy Rule and Security Rule. However, HHS has delegated much of its enforcement authority to the OCR. Although HIPAA and the HITECH Act typically refer to HHS, it is often OCR that actually will take the action. Accordingly, HHS and OCR are interchangeably referenced throughout this chapter.

HIPAA Privacy and Security Rules Prior to Amendment by HITECH

When it was first enacted, HIPAA directly governed only health plans, health care clearinghouses and health care providers who electronically

transmitted health information in certain standard transactions (Covered Entities). PL 104-191, 45 CFR § 164.104; *see also Covered Entity Charts—Guidance on how to determine whether an organization or individual is a covered entity under the Administrative Simplification provisions of HIPAA*, Centers for Medicare & Medicaid Services, <http://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf> (last visited July 28, 2011). The effective date of the Privacy Rule was April 14, 2003, for all Covered Entities, except small health plans, which were provided with additional time to comply. The effective date of the Security Rule was April 20, 2005, except small health plans, which were again provided additional time to comply.

The HIPAA Privacy Rule, as originally enacted, only governed uses and disclosures of individually identifiable health information by Covered Entities (“Protected Health Information,” or PHI). 45 CFR 164.104. The general rule is, unless specifically permitted by HIPAA, uses and disclosures of PHI require written patient authorization. 45 CFR 164.502. Some examples of permitted uses and disclosures without patient authorization include treatment, payment and health care operations purposes, and for certain other purposes, including as required by law, for certain public health purposes, for law enforcement purposes, among others 45 CFR §§ 164.506, 164.510 and 164.512.

The HIPAA Privacy Rule also provides individuals with certain rights, including the right to request certain restrictions and confidential communications of PHI, the right to access their PHI, the right to amend PHI, and the right to an account of certain disclosures of PHI, among others. 45 CFR §§ 164.522, 164.524, 164.526 and 164.528. The HIPAA Privacy Rule did not directly govern vendors and service providers of Covered Entities with access to PHI in order to perform services for, or create PHI on behalf of, Covered Entities. Rather, HIPAA required Covered Entities to contractually bind such third-party vendors and service providers, defined as “Business Associates,” to protect PHI and use and disclose PHI only as necessary to provide services to the Covered Entity. 45 CFR 164.502(e). Such contracts are defined as “Business Associate Agreements.”

Prior to the HITECH Act, the HIPAA Security Rule applied to electronic PHI (e-PHI) only in the possession of Covered Entities. Specifically, the Security Rule requires Covered Entities to ensure the confidentiality, integrity, and availability of e-PHI by implementing and maintaining certain administrative, physical, and technical safeguards.

Enforcement Prior to HITECH

The OCR is responsible for enforcing the HIPAA Privacy Rule and, as of July 27, 2009, the Security Rule. Prior to that time, the Centers for Medicare and Medicaid Services (CMS) was responsible for enforcing the Security Rule. Both CMS and OCR have been criticized for not vigorously enforcing the Privacy Rule or Security Rule.

Until recently, most Privacy and Security Rule violations were resolved without civil monetary penalties through voluntary compliance or settlement agreements. The government did not regularly conduct audits of Covered Entities. Most issues were resolved by Covered Entities responding to OCR complaints and implementing corrective action. There is no private right of action under HIPAA, so, prior to the HITECH Act, individuals could not recover money for HIPAA violations. Given the lack of penalties or other negative consequences for lack of compliance, HIPAA was often not a high-compliance priority.

HIPAA Privacy and Security Rule after Amendment by HITECH

The enforcement scope and penalties under HIPAA dramatically changed in 2009. On February 17, 2009, President Barack Obama signed into law the American Recovery and Reinvestment Act of 2009, PL 111-5 (ARRA), commonly referred to as the federal stimulus package. A significant portion of ARRA's stimulus expenditures and measures were related to health information technology (HIT) and incentives to adopt electronic health record (EHR) systems. ARRA, Section 13001, 42 USC 201. However, the government recognized that widespread adoption of HIT and EHR systems would not occur unless there was public assurance that the privacy and security of patient information in such systems were protected. In recognition of this, ARRA significantly expanded the scope of the privacy

and security requirements under HIPAA pursuant to the HITECH Act provisions within the ARRA.

The HITECH Act affected Covered Entities and their Business Associates by expanding the scope of the HIPAA Privacy and Security Rule to directly govern Business Associates, as well as Covered Entities. HITECH Act Sec. 13401(a) and 13404, 42 USC 17931. The HITECH Act imposed new security breach notification obligations on Covered Entities and Business Associates, requiring them to report breaches of unsecured PHI. HITECH Act, Section 13402, 42 USC 17932. In addition, the HITECH Act required Business Associates to report their security breaches to the applicable Covered Entities. The HITECH Act also imposed new requirements and strengthened existing requirements to provide increased protection to PHI (e.g., new restrictions on marketing, increased scope of accounting of disclosures, new prohibition on sale of PHI). HITECH Act Sec. 13405 and 13406, 42 USC 17935 and 17936. In addition, it required Covered Entities and their Business Associates to revise many of their policies and procedures and will likely require them to amend their Business Associate agreements. HITECH Act Sec. 13404(a) & (b), 42 USC 17934.

However, the provisions of the HITECH Act with the most significant, far-reaching impact were the mandatory breach notification requirements coupled with a new, heightened enforcement scheme. The potential exposure to Covered Entities for penalties, fines, and damages significantly increased under the HITECH Act. HITECH Act Section 13410, 42 USC 17939. Business Associates also are subject to the same heightened civil and criminal penalties that apply to Covered Entities. HITECH Act Section 13401, 42 USC 17931. In addition to increased penalties, the HITECH Act provides state attorneys general with enforcement authority to bring civil actions and obtain damages on behalf of their states' residents whose HIPAA rights have been violated. HITECH Act Section 13410(e), 42 USC 17939. Although there is still no private right of action, this change provides for some opportunity for individuals to recover damages. It is important to note that a recent case from the US District Court, Eastern District of Missouri held that notwithstanding the lack of a private right of action under HIPAA, disclosure of PHI in violation of HIPAA can form the basis for a state law negligence per se tort claim. *I.S. v. Washington Univ.*, No. 4:11CV235SNLJ, 2011 WL 2433585 (E.D. Mo. June 14, 2011).

Recent Guidance

On August 24, 2009, HHS published an Interim Final Rule to implement the new breach notification requirements (Breach Notification Rule). 74 Fed. Reg. 42740 (Aug. 24, 2009). To date, a Final Rule has not been published.

On October 30, 2009, HHS published an Interim Final Rule to implement the new enforcement provisions under the HITECH Act (Enforcement Rule). 74 Fed. Reg. 56123 (Oct. 30, 2009). To date, a Final Rule has not been published. However, additional changes were proposed in the Proposed Rule, which is described next.

On July 14, 2010, the OCR published a Proposed Rule to implement certain of the HITECH Act requirements (Proposed Rule). 75 Fed. Reg. 40868 (July 14, 2010). To date, a final rule has not been issued. The Proposed Rule contains a number of controversial requirements that, if finalized, will create significant compliance concerns (e.g., additional restrictions on marketing communications and sale of PHI).

On May 31, 2011, OCR issued a separate Proposed Rule to address changes to the accounting of disclosures requirements under the HITECH Act (Proposed Accounting Rule). 76 Fed. Reg. 31426 (May 31, 2011). The Proposed Accounting Rule would significantly expand this right to include the right to a report detailing all access to e-PHI. This would also create significant compliance concerns.

Further Notification and Enforcement Requirements

The HITECH Act promulgated the first breach notification requirements directly applicable to Covered Entities and their Business Associates. HITECH Act Section 13402, 42 USC 17932. Pursuant to the Breach Notification Rule, Covered Entities are required to report breaches of PHI or e-PHI to affected individuals, the OCR, and, in certain cases, the media. 45 CFR §§ 164.404, 164.406 and 164.408. Business Associates are required to report breaches to their Covered Entities. 45 CFR 164.410. Any use or disclosure of PHI or e-PHI not permitted by HIPAA may constitute a reportable breach. 45 CFR 164.402. These new requirements increase the

risk that a Covered Entity or Business Associate with a reportable breach will be subject to investigation and enforcement by the OCR and DOJ, as well as a civil action through the state attorneys general or a civil or criminal action based on state privacy law.

As mentioned above, the HITECH Act gave state attorneys general the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules. HITECH Act Sec. 13410(e), 42 USC 17939. The HITECH Act permits state attorneys general to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules. *Id.* The HITECH Act details how the amount of damages is to be calculated, including factors a court may consider to reduce the amount of damages. *Id.* Attorneys general may not bring an action during the time that an action for CMPs by HHS is pending. *Id.* OCR started offering HIPAA Enforcement Training in April 2011 to help state attorneys general and their staffs use their new authority to enforce the HIPAA Privacy and Security Rules. Health Information Privacy HHS.GOV, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html>. The training course will aid state attorneys general in investigating and seeking damages for HIPAA violations that affect residents of their states.

In response to criticism that HIPAA lacked enforcement, the HITECH Act mandates OCR, as part of HHS, to conduct periodic audits to ensure that Covered Entities and Business Associates are in compliance. HITECH Act Sec. 13411, 42 USC 17940.

In May 2011, the Federal Office of Inspector General issued two reports detailing its findings from HIPAA Security Rule audits at seven hospitals. The reports were very critical of OCR and called for it to ramp up its compliance review efforts to ensure adequate security controls. DANIEL R. LEVINSON, INSPECTOR GENERAL, AUDIT OF INFORMATION TECHNOLOGY SECURITY INCLUDED IN HEALTH INFORMATION TECHNOLOGY STANDARDS (MAY 2011), *available at* <http://oig.hhs.gov/oas/reports/other/180930160.pdf>.

Perhaps in response to these criticisms, including the Inspector General reports, HHS moved the HIPAA audit program forward recently. On June 9, 2011, HHS awarded a contract to Booz Allen Hamilton for \$180,000 to identify audit candidates. On June 10, 2011, HHS awarded a contract to KPMG for \$9.2 million to develop a HIPAA audit program and to conduct certain audits of Covered Entities and Business Associates by December 31, 2012. The specifics regarding HIPAA audits are still largely unknown. However, in a recent interview of Susan McAndrew, deputy director of OCR, published by HealthcareInfoSecurity.com McAndrew said the HIPAA compliance audit program will likely commence later in 2011 or early 2010 “after up to 20 test audits are completed... [and the] formal program for as many as 150 on-site audits will continue through the end of 2012.” Interview with Susan McAndrew, Deputy Director of the Federal Agency overseeing HIPAA Compliance Audit Program (July 15, 2011), *available at* http://www.healthcareinfosecurity.com/podcasts.php?podcastID=1190&rf=2011-07-15-h&hq_e=el&hq_m=1202736&hq_l=5&hq_v=2ccc3bb082. McAndrew indicated that the audit program will be used to help ensure compliance but could also be used as an enforcement tool. McAndrew also indicated that OCR is testing an onsite audit model, but that entities would receive advance notice of audits, along with document requests. Covered Entities and Business Associates should proactively follow the developing information regarding the HIPAA audit process.

To anticipate these pending HIPAA audits, Covered Entities need to immediately review and, if necessary, update their HIPAA Privacy and Security compliance programs in light of the new HIPAA enforcement efforts by the OCR. It had previously appeared that Business Associates had been given a surprising unofficial pass on enforcement actions until the final HIPAA rules are issued, according to Sue McAndrew. Specifically, she stated in a recent HIPAA Summit in DC that “[c]urrently, any enforcement actions against business associates would await the promulgation of the final rulemaking, which carries with it the regulatory structure for BAs to assume the liability from the HITECH Act.” *During ‘Limbo,’ CEs Should Tighten Their Oversight of BAs, Enhance Protections*, REPORT ON PATIENT PRIVACY, *reprinted in* 11 HEALTH BUS. DAILY 5, May 2011, at 8. However, more recently, McAndrew stated that OCR had not yet determined whether audits would include Business Associates and

the KPMG protocols will support Business Associate audits. *See supra* Interview with Susan McAndrew.

Security Rule Enforcement Facts

- Since OCR began reporting its Security Rule enforcement results in October 2009, HHS has received approximately 420 complaints alleging a violation of the Security Rule. According to the OCR, during this period, it closed 192 complaints after investigation and appropriate corrective action. As of May 31, 2011, OCR had 294 open complaints and compliance reviews. See OCR, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/index.html> (last visited July 14, 2011)

Privacy Rule Enforcement Facts

- Since the compliance date in April 2003, HHS has received more than 61,333 HIPAA Privacy complaints. HHS resolved more than 91 percent of complaints received (more than 55,858): through investigation and enforcement (more than 13,745); through investigation and finding no violation (7,132); and through closure of cases that were not eligible for enforcement (40,456). The following is more detail on these statistics.
- HHS through OCR has investigated and resolved more than 13,745 cases by requiring changes in privacy practices and other corrective actions by Covered Entities. It is HHS's position that these corrective actions have resulted in change that is systemic and that affects all individuals. According to HHS, it has successfully enforced the Privacy Rule by applying corrective measures in all cases where an investigation indicates noncompliance by the Covered Entity. OCR has investigated complaints against many different types of entities, including national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.
- In another 7,132 cases, HHS/OCR investigations found that no violation had occurred.
- For the remainder of HHS's completed cases (40,456), HHS determined that the complaint did not present an eligible case for

enforcement of the Privacy Rule. Reasons a case was not eligible for enforcement include:

- OCR lacked jurisdiction under HIPAA (e.g., a complaint alleged a violation prior to the Privacy Rule compliance date or alleged a violation by an entity not covered by the Privacy Rule).
- The complaint was untimely, or withdrawn, or not pursued by the filer.
- The activity described did not violate the Privacy Rule (e.g., the Covered Entity has disclosed protected health information in circumstances in which the Rule permits such a disclosure).

According to OCR, the compliance issues investigated most are, in order of frequency:

1. Impermissible uses and disclosures of protected health information
2. Lack of safeguards of protected health information
3. Lack of patient access to their protected health information
4. Uses or disclosures of more than the minimum necessary protected health information
5. Complaints to the Covered Entity

The most common types of Covered Entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:

1. Private physician practices
2. General hospitals
3. Outpatient facilities
4. Health plans (group health plans and health insurance issuers)
5. Pharmacies

Health Information Privacy, HHS.GOV, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/index.html> (last visited July 14, 2011) *See also Numbers at a Glance*, HHS.GOV (May 31, 2011), <http://www.hhs.gov/ocr/>

privacy/hipaa/enforcement/highlights/indexnumbers.html, showing graphs of the status of all privacy complaints, total investigated resolutions, and investigated resolutions between April 14, 2003 and April 30, 2011.

Compliance Concerns

Understanding and Preventing Security Breaches

Security breaches are currently one of the areas posing the greatest compliance concerns because of the costs associated with responding to large breaches, as well as the resulting negative publicity. According to the Ponemon Institute, it costs approximately \$214 per affected individual to respond to a security breach. *Cost of a Data Breach Climbs Higher*, PONEMON INSTITUTE (March 8, 2011), <http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher>. It is not uncommon for breaches, especially those involving electronic information, to affect hundreds of thousands of individuals, if not more. See discussion below for examples of large security breaches. The larger the breach, the more negative publicity is generated. In addition to the HIPAA Breach Notification Rule, there are breach notification requirements at the state level. To the extent that these laws are more protective of patient privacy, they are not preempted by HIPAA. As a result, state laws must be considered when responding to any security breach.

State laws vary widely in the scope of information they cover and their notification requirements. Some state laws require notification only to affected individuals, and the requirements governing the content of such notifications are not materially different from what is required by the HIPAA Breach Notification Rule. *See*, e.g., Arizona, AZ ST § 44-7501, Illinois, 815 ILCS 530/5.1. However, other states may require additional notification to certain state officials. *See* e.g., California, Health & Safety Code section 1280.15; Massachusetts, Mass. Gen. Laws Ch. 93H, §§ 1-6. Some may also have unique requirements regarding the content of notifications to affected individuals. *See* e.g., Maryland, Md. Code Ann. Com. Law §§ 14-3504-3508. These state law requirements can significantly add to the compliance burden involved in responding to a security breach, especially if the breach involves affected individuals from many different states.

The best way to prevent security breaches is to advise clients to secure PHI in accordance with the Guidance issued by the OCR to the extent possible. *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, HHS. GOV, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html> (last visited July 28, 2011). The Guidance endorses the standards of the National Institute of Standards and Technology (NIST) for encrypting and destroying data. Securing PHI in accordance with the Guidance is the single most effective way to reduce the risk of penalties because such data is not subject to the Breach Notification Rule. Further, because many of the largest breaches have been caused by Business Associates, rather than Covered Entities, it is important that Covered Entities review and revise, if necessary, their Business Associate Agreements to address responsibility for costs associated with reporting a breach, as well as to address the security practices of Business Associates. Finally, before reporting a breach, it is important to contact legal counsel to ensure the incident actually constitutes a breach that is required to be reported by HIPAA and/or state law.

Privacy Compliance and Implementation of Interoperable Electronic Health Records

As discussed above, a significant portion of ARRA's stimulus expenditures and measures were related to incentives to adopt interoperable EHR systems. The policy behind the government's decision to use financial incentives to forward the adoption and implementation of these systems includes the perceived cost savings associated with use of such systems to increase quality of care and decrease medical errors. Interoperable EHR systems are thought to help to achieve these goals because any treating health care provider, regardless of location, would be able to access all of the patient's medical records. All information about the patient's medical history, medication allergies, and drug history would be in the provider's hands with the touch of a few keys. However, the privacy issues that must be addressed when implementing such systems can be complex.

Although the changes to HIPAA through the HITECH Act have increased the risks associated with noncompliance, the HIPAA privacy standards remain uniform, apply nationally, and permit broad access to medical records for treatment purposes without prior patient consent. This uniformity makes implementation of an interoperable EHR system much

easier. In contrast, each state has its own privacy laws, which, if more protective of patient privacy, are not preempted by HIPAA. 45 CFR 160 Subpart B.¹

Privacy laws across multiple states can impose complex and often inconsistent or conflicting standards that must be met to successfully implement an interoperable EHR system. The state laws governing more sensitive types of health information—e.g., HIV test results, mental health/developmental disabilities information, genetic information, alcohol and drug abuse treatment records—are almost always more stringent than HIPAA. *See e.g.*, Illinois Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/1; Wisconsin Confidentiality of HIV Test Results, Wis. Stat. 252.15. These laws often impose restrictions that conflict with the most routine types of information sharing that are permitted under HIPAA, such as sharing for purposes of treatment or for obtaining payment. As a result, while HIPAA would permit these sensitive types of records to be put into an EHR and accessed for treatment and certain other purposes, it may be problematic under state law to do so.

In addition, other federal privacy laws and regulations impose unique requirements affecting the incorporation of covered information into an EHR system. Examples include the Federal Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR § 2, which strictly protects the confidentiality of certain alcohol and drug abuse treatment records, and the Department of Transportation (DOT) regulations that govern records generated from certain occupational health tests and examinations. 49 CFR § 40. The federal agency that enforces 42 CFR § 2, the Substance Abuse and Mental Health Services Administration (SAMHSA), has affirmatively addressed this issue through guidance. SARAH A. WATTENBERG, LEGAL ACTION CTR. FOR THE SUBSTANCE ABUSE & MENTAL HEALTH SERVS., FREQUENTLY ASKED QUESTIONS APPLYING THE SUBSTANCE ABUSE CONFIDENTIALITY REGULATIONS TO HEALTH INFORMATION

¹ In general, state laws that are contrary to the Privacy Rule are preempted by the Privacy Rule, which means that the Privacy Rule will apply. “Contrary” means that it would be impossible for a Covered Entity to comply with both the state and federal requirements, or that the provision of state law is an obstacle to accomplishing the full purposes and objectives of HIPAA. The Privacy Rule provides exceptions to the general rule of federal preemption for contrary state laws. 45 CFR 160.203.

EXCHANGE (HIE) available at <http://www.samhsa.gov/HealthPrivacy/docs/EHR-FAQs.pdf> (last visited July 28, 2011). According to SAMHSA, alcohol and drug abuse treatment records governed by 42 CFR § 2 can be put into EHR systems. However, because the ability to access such records for treatment purposes is restricted to circumstances where there is a medical emergency, the records must be segregated through technology, commonly referred to as “break the glass” functionality. Although possible, implementation of such additional functionality can be burdensome and costly. However, failure to take additional steps to protect records in accordance with the conflicting requirements of all applicable laws creates significant risk.

Risks associated with noncompliance with HIPAA, as well as these other various more stringent legal requirements, range from adverse public relations and business reputation consequences to serious financial repercussions, including fines and penalties. It is important to emphasize that some of these laws, including HIPAA, can impose criminal penalties for violations (e.g., HIPAA, 42, USC § 1320d-6; 42 CFR § 2.4; California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.36).

Recent Enforcement Actions by OCR

The following are examples of recent actions by OCR. For information on other OCR actions, see *Enforcement Data*, HHS.GOV, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/index.html> (last visited July 14, 2011). These actions illustrate the new enforcement environment of HIPAA privacy and security. It is important to note that this area is rapidly changing, and enforcement actions continue to occur.

Cignet

On February 22, 2011, OCR issued a Notice of Final Determination finding that Cignet Health of Prince George’s County, Maryland (Cignet), violated the Privacy Rule. HHS imposed a civil money penalty (CMP) of \$4.3 million for the violations. This was the first CMP issued by HHS for violations of the HIPAA Privacy Rule. According to HHS, the amount of

the CMP was based on the violation categories and increased penalty amounts authorized by Section 13410(d) of the HITECH Act.

In a Notice of Proposed Determination (NPD) issued October 20, 2010, OCR found that Cignet violated forty-one patients' rights by denying them access to their medical records. These patients, each of whom made a request to obtain their record between September 2008 and October 2009, individually filed complaints with OCR, initiating investigations of each complaint. The HIPAA Privacy Rule requires that a Covered Entity provide a patient with a copy of his or her medical records within thirty (and no later than sixty) days of the patient's request. The CMP for these violations was \$1.3 million.

During the investigations, Cignet refused to respond to OCR's repeated demands to produce the records. Additionally, Cignet failed to cooperate with OCR's investigations of the complaints, including failure to produce the records in response to OCR's subpoena. OCR filed a petition to enforce its subpoena in US District Court and obtained default judgment against Cignet on March 30, 2010. On April 7, 2010, HHS assessed a \$1.3 million CMP against Cignet for its violations of the HIPAA Privacy Rule. HHS also assessed a \$3 million CMP on the grounds that Cignet failed to cooperate in OCR's investigation. Covered Entities are legally required under 45 CFR § 160.310(b) to cooperate with the government in such investigations. Yet, according to OCR's findings, Cignet failed to cooperate with OCR's investigations of the complaints, and Cignet did not produce the records in a timely manner in response to OCR's requests.

Cignet eventually produced the medical records to OCR, but according to OCR, Cignet made no efforts to resolve informally the complaints with the patients or the government. The lesson to be learned from this action is that it is critical to respond to both complaints from individuals and government investigations.

Massachusetts General Hospital

On February 14, 2011, HHS entered into a Resolution Agreement with The General Hospital Corporation and Massachusetts General Physicians Organization Inc. (Mass General) to settle potential violations of the HIPAA Privacy and Security Rules. In the agreement, Mass General agreed

to pay \$1,000,000 and enter into a Corrective Action Plan (CAP) to implement policies and procedures to safeguard the privacy of its patients. The incident giving rise to the agreement involved the loss of PHI of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. Unlike the Cignet action, there were no allegations or CMPs imposed for willful neglect.

Enforcement Action Takeaways

HIPAA compliance is moving up on the ladder of compliance risks. In the past, many organizations were reluctant to provide resources for HIPAA compliance because there was no material enforcement, so it was not perceived as an area of real risk. That is beginning to change. Lawyers will be more involved in responding to breaches and counseling clients that are subject to complaints or OCR compliance reviews.

Navigating Enforcement Practices

The sections within the HIPAA regulations that address enforcement are found at 45 CFR § 160, subpart C (Compliance and Investigations), subpart D (Imposition of Civil Money Penalties), and subpart E (Procedures for Hearings). These rules are referred to collectively as the "Enforcement Rule." As noted above, the Enforcement Rule was modified by the 2009 Interim Final Rule, and further changes are proposed in the 2010 Proposed Rule.

The Enforcement Rule first sets forth the process for filing complaints with the OCR. Then, the Enforcement Rule states the process the OCR must follow when investigating complaints it receives and conducting compliance reviews. Next, the Enforcement Rule sets forth the basis for imposition of a civil money penalty, how such penalties will be calculated, affirmative defenses, and the processes for proposing penalties and collecting penalties. Last, the Enforcement Rule addresses administrative hearings relating to imposition of civil monetary penalties and the appeals process.

The Right to File a Complaint

Any person who believes a Covered Entity or Business Associate is not complying with the administrative simplification provisions may file a complaint with the secretary. 45 CFR 160.306(a). Complaints must:

1. Be filed in writing, either on paper or electronically
2. Name the person who is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s)
3. Be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the secretary for good cause shown.

45 CFR 160.306(b)(1-3). The secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register. 45 CFR 160.306(b)(4).

Complaint Investigation and Compliance Reviews

OCR is responsible for enforcing HIPAA. OCR carries out this responsibility in several different ways. One way is to investigate a complaint. The HITECH requires the OCR to investigate any complaint filed when the preliminary facts indicate a possible violation due to willful neglect. HITECH Act Sec. 13410(c)(2), 42 USC 17939. The OCR may, but is not required to, investigate other complaints not due to willful neglect. 45 CFR 160.306(c)(2). OCR's investigation may include a review of pertinent policies, procedures, or practices of the Covered Entity or Business Associate and of the circumstances regarding any alleged violation. 45 CFR 160.306(c)(3). At the time of the initial written communication with the Covered Entity or Business Associate about the complaint, the OCR will describe the acts and omissions that are the basis of the complaint. 45 CFR 160.306(c)(4).

Another way OCR enforces HIPAA is to conduct compliance reviews to determine whether Covered Entities and Business Associates are in compliance with HIPAA. The OCR may, but is not currently required to, conduct a compliance review to determine whether a Covered Entity or Business Associate is complying with HIPAA. 45 CFR 160.308. The OCR has indicated that it will conduct a compliance review of a Covered Entity when it is notified by a Covered Entity of a security breach affecting more than 500 individuals. *OCR Pushes 'Culture of Compliance,' Shares Data on Breaches, Investigations*, REPORT ON PATIENT PRIVACY, reprinted in 11 HEALTH BUS.

DAILY 4, April 2011, <http://aishealth.com/archive/hipaa0411-01>. The HITECH Act also requires the Secretary of HHS to provide for periodic audits to ensure that Covered Entities and Business Associates are complying with HIPAA. HITECH Act Sec. 13411, 42 USC 17940.

The OCR may issue subpoenas to require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review. 45 CFR 160.314(a); *see also*, 42 USC 405(d) and (e), 1320a-7a(j), and 1320d-5. For the specific subpoena requirements and who may serve the subpoena, refer to 45 CFR 160.314 (a) (1 & 2). In addition, the Enforcement Rule sets forth the permissible procedures to be followed during an investigational proceeding, which is a non-public proceeding. 45 CFR 160.314(b). Such procedures include requiring testimony to be made under oath and requiring objections to be asserted on the record. 45 CFR 160.314(b)(1). Investigational proceedings are recorded and transcribed. 45 CFR 160.314(b)(8). In general, witnesses are entitled to copies of the record, except, for good cause, they may be limited to inspection of their own testimony only. *Id.* Witnesses may propose corrections to the record. 45 CFR 160.314(b)(9). All testimony and evidence that HHS obtains as part of an investigational inquiry may be used in any administrative or judicial proceeding. 45 CFR 160.314(c).

In addition, to the extent practical, the OCR will seek the cooperation of Covered Entities and may provide technical assistance to help them comply voluntarily with HIPAA. 45 CFR 160.304, 42 USC 17933. OCR also performs education and outreach to foster compliance with requirements of the Privacy and Security Rules. *Id.* HITECH requires the OCR to issue guidance annually on the most effective and appropriate technical guidance to meet the requirements of the Security Rule. HITECH Act Sec. 13401, 42 USC 17931. *See also* *Enforcement Process*, HHS.GOV, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html> (last visited July 28, 2011).

What OCR Considers During Intake and Review of a Complaint

OCR reviews the complaints it receives from individuals, and it may take action on only certain complaints. The OCR states on its website that the

following factors are what it considers during intake and review of a complaint. See *What OCR Considers During Intake & Review*, HHS. Gov, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/whatocrconsiders.html> (last visited July 28, 2011).

First, the alleged action must have taken place after the dates the Privacy Rule took effect. Compliance with the Privacy Rule was not required until April 14, 2003. Compliance with the Security Rule was not required until April 20, 2005. Therefore, OCR cannot investigate complaints about actions that took place before these dates.

Second, the complaint must be filed against an entity that is required by law to comply with the Privacy and Security Rules. This means that the complaint must be against a Covered Entity or Business Associate. Not all organizations are covered by the Privacy and Security Rules. The following are some examples of organizations that are not required to comply with HIPAA unless they otherwise qualify as a Business Associate: life insurers, employers (self-insured plans are required to comply), workers compensation carriers, schools and school districts, state agencies (e.g., child protective service agencies), law enforcement agencies, and municipal offices.

Third, a complaint must allege an activity that, if proven true, would violate the Privacy or Security Rule. For example, OCR would not investigate a complaint that alleged that a physician sent a person's demographic information to an insurance company to obtain payment because the Privacy Rule generally permits doctors to use and disclose such information to bill for their services.

Fourth, complaints must be filed within 180 days of when the person submitting the complaint knew or should have known about the alleged violation of the Privacy or Security Rule. OCR may waive this time limit if it determines that the person submitting the complaint shows good cause for not submitting the complaint within the 180-day time frame, such as circumstances that made submitting the complaint within 180 days impossible.

If OCR accepts a complaint for investigation, OCR will notify the person who filed the complaint and the Covered Entity or Business Associate named in it. Then, the complainant and the Covered Entity or Business Associate are asked to present information about the incident or problem described in the complaint. OCR may request specific information from each to get an understanding of the facts. Covered entities are required by law to cooperate with complaint investigations. 45 CFR 160.310.

If a complaint describes an action that could be a violation of the criminal provision of HIPAA, 42 U.S.C. 1320d-6, OCR may refer the complaint to the Department of Justice for investigation.

OCR then reviews the information, or evidence, that it gathers in each case. After an investigation or compliance review, if the OCR determines that further action is not warranted, the OCR will inform the Covered Entity or Business Associate, and if the matter arose from a complaint, the complainant, in writing. 45 CFR 160.312(b). If the evidence indicates that the Covered Entity or Business Associate was not in compliance, OCR will attempt to resolve the case with the Covered Entity or Business Associate by obtaining:

- Voluntary compliance
- Corrective action
- Resolution agreement

45 CFR 160.312(a)(1).

In the past, most investigations have been concluded to the satisfaction of OCR through these types of resolutions. If the matter is resolved through one of these informal means, the OCR must notify the person who filed the complaint and the Covered Entity or Business Associate in writing of the resolution result. 45 CFR 160.312(a)(2).

If the matter is not resolved through one of these informal means, the OCR will inform the Covered Entity or Business Associate and provide the Covered Entity or Business Associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration. 45 CFR 160.312(a)(3). The Covered Entity or Business Associate must

submit the evidence to the OCR within thirty days of receipt of such notification. 45 CFR 160.312(a)(3)(i). If the OCR finds that a civil monetary penalty should be imposed, it must inform the Covered Entity or Business Associate of such finding in a notice of proposed determination. 45 CFR 160.312(a)(3)(ii). The following describes the requirements of a notice of proposed determination.

Notice of Proposed Determination

The notice of proposed determination must include:

1. Reference to the statutory basis for the penalty
2. A description of the findings of fact regarding the violations with respect to which the penalty is proposed (except that, in any case where the OCR is relying upon a statistical sampling study in accordance with 45 CFR 160.536, the notice must provide a copy of the study relied upon by the OCR)
3. The reason(s) the violation(s) subject(s) the respondent to a penalty
4. The amount of the proposed penalty and a reference to the section in the Enforcement Rule's provisions on calculating CMPs (45 CFR 160.404) upon which the proposed penalty amount was based
5. Any circumstances that were considered in determining the amount of the proposed penalty
6. Instructions for responding to the notice, including a statement of the respondent's right to a hearing, a statement that failure to request a hearing within ninety days permits the imposition of the proposed penalty without the right to a hearing or a right of appeal, and the address to which the hearing request must be sent

45 CFR 160.420(a)(1-6).

Response to Notice of Proposed Determination

The respondent may request a hearing before an administrative law judge (ALJ) on the proposed penalty. 45 CFR 160.420(b). The process to request a hearing before an ALJ on the proposed penalty is set forth in the Section titled "Procedures for Hearings," below. If the respondent does not request

a hearing within the time required under 45 CFR Sec. 160.504, and the matter is not settled with HHS as described above, the OCR will impose the proposed penalty or any lesser penalty permitted by 42 U.S.C. 1320d-5. 45 CFR 160.422. The OCR will notify the respondent by certified mail, return receipt requested, of any penalty that has been imposed and of the means by which the respondent may satisfy the penalty, and the penalty is final on receipt of the notice. *Id.* The respondent has no right to appeal a penalty under 45 CFR 160.548 with respect to which the respondent has not requested a hearing in a timely manner. *Id.*

Imposition of Civil Money Penalties

If the Covered Entity or Business Associate does not take action to resolve the matter in a way that is satisfactory, OCR may recommend imposing civil money penalties (CMPs) on the Covered Entity or Business Associate. 45 CFR 160.402. If CMPs are imposed, the Covered Entity or Business Associate may request a hearing in which an HHS administrative law judge decides whether the penalties are supported by the evidence in the case. 45 CFR 160.546. Complainants do not receive a portion of CMPs collected from Covered Entities or Business Associates; the penalties are deposited in the US Treasury and then transferred to the OCR for purposes of enforcing HIPAA. HITECH Act Sec. 13410(e), 42 USC 17938. HITECH also requires the OCR to establish, by regulation, a methodology under which an individual who is harmed because of a HIPAA violation may receive a percentage of any CMP or monetary settlement collected with respect to such offense. HITECH Act Sec. 13410(c)(3) & (4), 42 USC 17938.

Who Can Be Liable for Civil Money Penalties

1. Covered Entities and Business Associates. Covered Entities and Business Associates can be liable for CMPs if they violate HIPAA. 45 CFR 160.402(a), HITECH Act Sec. 13401(b) and 13404(c), 42 USC 17931 and 17934. Violations by employees or other workforce members or agents of a Covered Entity are attributed to the Covered Entity if the individual was acting in the scope of employment or agency. 45 CFR 160.402(c). Prior to HITECH, Covered Entities were not liable for Business

Associates, even those considered to be agents if there was an appropriate Business Associate Agreement and the Covered Entity did not know of a pattern or practice of noncompliance by the Business Associate that the Covered Entity failed to act upon. 45 CFR 164.504(e). Questions remained as to whether individuals who were not Covered Entities could be liable for violations of HIPAA. The Enforcement Rule provides that only a Covered Entity is liable for a civil money penalty. 45 CFR 160.4021. However, HITECH clarified that although persons (including employees or other individuals) who are not Covered Entities or Business Associates cannot be held liable for CMPs, they can be liable for criminal penalties under HIPAA. HITECH Act Sec. 13409, 42 USC 17938.

2. Affiliated Covered Entities. Certain organizational designations can affect liability. A Covered Entity that is a member of an affiliated Covered Entity may have joint and several liability with the other Covered Entities in its group. 45 CFR 160.402(b)(2). An affiliated Covered Entity is a group of Covered Entities under common ownership or control that have elected to be treated as if they were one Covered Entity for purposes of compliance with the Security and Privacy Rules. 45 CFR 164.105(b). Affiliated Covered Entities will be jointly and severally liable for a civil money penalty for a violation, 45 CFR 160.402(b)(1), unless it is established that another member of the affiliated Covered Entity was responsible for the violation. 45 CFR 160.402(b)(2).

Criminal Penalties and CMPs

Persons who commit certain violations of the Privacy Rule may be subject to criminal penalties. In addition, Covered Entities and Business Associates that fail to comply voluntarily with HIPAA may be subject to CMPs.

Criminal Penalties

A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal

penalty of up to \$50,000 and up to a one-year imprisonment. 42 USC 1320d-6(b)(1). The criminal penalties increase to \$100,000 and up to five years' imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to ten years' imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain, or malicious harm. 42 USC 1320d-6(b)(20-3). A "person" means "a natural person, trust or estate, partnership, corporation, professional association or corporation or other entity, public or private." 45 CFR 160.103. The Department of Justice (DOJ) is responsible for criminal prosecutions under the Privacy Rule and historically prosecuted only a small number of criminal HIPAA violations. However, in June 2011, the DOJ increased its enforcement efforts by obtaining two indictments in HIPAA criminal cases. See *United States v. Kaye*, No. 2:11-CR-00099 (E.D. Va. filed June 21, 2011); *United States v. Stewart*, No. 2:11-CR-00254 (N.D. Ala. filed June 28, 2011). See also "DOJ Steps Up Enforcement with Indictment of 'Loose Lips' Doctor, Hospital Visitor," 11 Report on Patient Privacy 7 (July 2011).

Civil Money Penalties

As discussed above, CMPs may be imposed on Covered Entities and Business Associates for a failure to comply with the Privacy Rule and Security Rule. On October 30, 2009, the Department of Health and Human Services adopted the Enforcement Rule as an Interim Final Rule implementing the HITECH Act's "improved enforcement" provisions. 74 Fed. Reg. 56123 (Oct. 30, 2009). The Enforcement Rule significantly increased the penalty amounts that may be imposed for HIPAA violations and established a tiered system for CMPs reflecting increasing levels of culpability and a range of penalty amounts. 45 CFR 160.404; 74 Fed. Regs. 56123, 56131. CMPs will vary significantly, depending on factors such as the date of the violation, whether the Covered Entity knew or should have known of the failure to comply, or whether the Covered Entity's failure to comply was due to willful neglect. *Id.* Penalties may not exceed a calendar year cap for multiple violations of the same requirement. *Id.* The following summarizes these penalties. 45 CFR 160.404, 74 Fed. Regs. 56123, 56131.

For violations occurring prior to February 18, 2009:

Penalty for Each Violation	Possible Total Penalty for Multiple Violations of Identical Provision in a Calendar Year
Up to \$100 per violation	\$25,000

For violations occurring on or after February 18, 2009:

Violation Category	Penalty for Each Violation	Possible Total Penalty for Multiple Violations of Identical Provision in a Calendar Year
<i>Did Not Know</i> (was unaware and could not have known if exercised reasonable diligence)	\$100–\$50,000	\$1,500,000
<i>Reasonable Cause</i> and not willful neglect	\$1,000–\$50,000	\$1,500,000
<i>Willful Neglect—Corrected</i> (violation due to willful neglect but was corrected after discovery in a timely manner)	\$10,000–\$50,000	\$1,500,000
<i>Willful Neglect—Not Corrected</i> (violation due to willful neglect and not corrected in a timely manner after discovery)	\$50,000	\$1,500,000

Violation Categories

- **Reasonable cause.** This is defined as “circumstances that make it unreasonable for the Covered Entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.” 45 CFR 160.401; 74 Fed. Regs. 56123, 56130. Note that although this definition was

not changed under the Interim Final Enforcement Rule, changes were proposed under the Proposed Rule to implement the HITECH Act, as follows: “Reasonable cause” means an act or omission in which a Covered Entity or Business Associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the Covered Entity or Business Associate did not act with willful neglect. 75 Fed. Regs. 40868, 40914 (July 14, 2010).

- Reasonable diligence. This is defined as “the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.” 45 CFR 160.401.
- Willful neglect. This is defined as “conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.” *Id.*

Affirmative Defenses

Under the Enforcement Rule, HHS is not permitted to impose a CMP if the Covered Entity or Business Associate can establish an affirmative defense, as follows:

For Violations Occurring Prior to February 18, 2009:

1. The violation is a criminal act punishable under 42 U.S.C. 1320d–6;
2. The Covered Entity establishes that it did not have knowledge of the violation (determined in accordance with the federal common law of agency), and, by exercising reasonable diligence, would not have known that the violation occurred;
3. The violation is due to reasonable cause and not willful neglect; and is corrected during either the thirty-day period beginning on the first date the Covered Entity knew, or by exercising reasonable diligence would have known, that the violation occurred (unless the period is extended at the discretion of HHS). 45 CFR 160.410(a).

For Violations Occurring On or After February 18, 2009:

1. The violation is a criminal act punishable under 42 U.S.C. 1320d–6;

2. The Covered Entity or Business Associate establishes that the violation is not due to willful neglect, and is corrected during either the thirty-day period beginning on the first date the Covered Entity or Business Associate knew, or, by exercising reasonable diligence, would have known that the violation occurred (unless the period is extended at the discretion of HHS). 45 CFR 160.410(b).

The Proposed Rule to implement the HITECH Act would change the affirmative defenses, including restricting the affirmative defense that the violation is punishable as a criminal offense, to apply only if a criminal penalty has actually been imposed. 75 Fed. Regs. 40868, 40915 (July 14, 2010). However, to date, a Final Rule has not been issued.

Ignorance will not bar a penalty for “willful neglect,” which is defined as a “conscious,” “intentional,” or “reckless indifference” to HIPAA obligations. It remains to be seen how the Enforcement Rule will be ultimately modified. In the meantime, Covered Entities and Business Associates need to implement a proactive and responsive HIPAA compliance program.

Waiver, Statute of Limitations, and Settlement

In addition to the affirmative defenses, HHS has certain discretionary authority regarding imposition of CMPs. For example, HHS may waive a CMP, in whole or part, if the failure to comply was due to reasonable cause and not willful neglect, and the penalty would be excessive, given the nature and extent of the violation. 45 CFR 160.412. HHS also has the discretion to settle any case and to reduce a CMP. HITECH Act Section 13410(c)(1), 42 USC 17939. However, under the HITECH act, willful neglect will result in a mandatory CMP. In addition, if a preliminary investigation indicates that a violation may be the result of willful neglect, there must be a formal investigation. *Id.* at Section 13410(c)(2).

There is a six-year statute of limitations for enforcement actions. 45 CFR 160.414.

Under the Enforcement Rule, before HHS imposes a penalty, it will notify the Covered Entity and provide the Covered Entity with an opportunity to provide written evidence of those circumstances that would reduce or bar a

penalty. 45 CFR 160.312(a)(3). This evidence must be submitted to HHS within thirty days of receipt of the notice. In addition, if HHS states that it intends to impose a penalty, a Covered Entity has the right to request an administrative hearing to appeal the proposed penalty. 45 CFR 160.420(b).

Whenever a proposed penalty becomes final, notification will go to the public and certain organizations and entities, including the appropriate state or local medical or professional organization, the appropriate state agency or agencies administering or supervising the administration of state health care programs, and the appropriate state or local licensing agency or organization. 45 CFR 160.426.

Procedures for Hearings

The regulations governing hearings provide a “respondent” with the right to request a hearing before an administrative law judge to address the imposition of CMPs. Section 45 CFR 160.302 currently defines a respondent as any Covered Entity upon which HHS has imposed or proposes to impose CMPs. This definition has been broadened under the HITECH Act to include Business Associates. HITECH Act Sections 13401 and 13404, 42 USC 17931 and 17934.

A request for a hearing must both be filed in a timely manner and meet each requirement of 45 CFR 164.504. The following describes these requirements.

1. The request for a hearing must be made in writing signed by the respondent or by the respondent’s attorney and sent by certified mail, return receipt requested, to the address specified in the notice of proposed determination. 45 CFR 160.504(b).
2. The request for a hearing must be mailed within ninety days after notice of the proposed determination is received by the respondent. The respondent’s date of receipt of the notice of proposed determination is presumed to be five days after the date of the notice unless the respondent makes a reasonable showing to the contrary to the ALJ. *Id.*
3. The request for a hearing must clearly and directly admit, deny, or explain each of the findings of fact contained in the notice of

proposed determination with regard to which the respondent has any knowledge. If the respondent has no knowledge of a particular finding of fact and so states, the finding shall be deemed denied. 45 CFR 160.504(c).

4. The request for a hearing must also state affirmative defenses and the factual and legal basis for opposing the penalty (except as noted above, a respondent may at any time raise the affirmative defense that the act is a criminal act for which CMPs cannot be imposed. 45 CFR 160.410(b)(1). *Id.*

An ALJ must dismiss a hearing request under the following circumstances:

1. On motion of the secretary, the ALJ determines that the respondent's hearing request is not filed in a timely manner or the hearing request does not contain all of the required elements for a valid hearing request. 45 CFR 160.504(d)(1).
2. The respondent withdraws the request for a hearing; 45 CFR 160.504(d)(2).
3. The respondent abandons the request for a hearing; or 45 CFR 160.504(d)(3).
4. The respondent's hearing request fails to raise any issue that may properly be addressed in a hearing. 45 CFR 160.504(d)(4).

Rights of the Parties, Discovery, and other Pre-Hearing Matters

The Enforcement Rule provides each of the parties with certain rights, such as the right to participate in any conference held by the ALJ and the right to present evidence and to present and cross-examine witnesses. 45 CFR 160.506. The parties also have the right to conduct document discovery, but do not have the right to full discovery, such as written interrogatories or depositions. 45 CFR 160.516(a) and (c). Discovery requests must be fully responded to within thirty days, or the party must respond with an objection and include the basis for the objection. 45 CFR 160.516(e)(1). In the event of an objection, the requesting party has thirty days to file a motion with the ALJ for an order compelling discovery. *Id.* The ALJ may extend any of the discovery periods. 45 CFR 160.516(e)(3).

The Enforcement Rule prohibit ex parte contacts with the ALJ (45 CFR 160.510); however, there is the opportunity to communicate with the ALJ prior to the hearing because the ALJ must schedule at least one prehearing conference and may schedule additional prehearing conferences upon no less than fourteen days' notice. 45 CFR 160.512. The prehearing conference may be used, for example, to simplify the issues, to discuss stipulations and admissions of fact, to discuss whether a party chooses to waive appearance at an oral hearing and to submit only documentary evidence (subject to the objection of the other party) and written argument, or to limit the number of witnesses. 45 CFR 160.512. The prehearing can be used to discuss the potential for the settlement of the case and other matters, including the protection of the privacy of individually identifiable health information that may be submitted into evidence or otherwise used in the proceeding. *Id.*

The Enforcement Rule requires the parties to exchange witness lists and copies of written statements or other documents to be introduced into evidence at least fifteen days before the hearing date, but not more than sixty days before such date. 45 CFR 160.518. If the respondent intends to introduce a statistical expert's report, it must be provided to the HHS party not less than thirty days before the hearing date. *Id.* The ALJ must decide upon any objections to witnesses or documents. 45 CFR 160.518(b)(1). Absent extraordinary circumstances, the ALJ will exclude from the hearing any witnesses or documents that are not provided in advance, as required under the Enforcement Rule. 45 CFR 160.518(b)(2).

The Enforcement Rule permits parties to make a motion to request the ALJ to issue a subpoena to compel an individual's appearance and testimony at the hearing, including production of relevant and material evidence. 45 CFR 160.520. A subpoena request must be made by written motion at least thirty days before the hearing date. 45 CFR 160.520(d). Objections to such motion must be filed within fifteen days after the motion is served. 45 CFR 160.520(f).

The Enforcement Rule specifically addresses other procedural aspects of the pre-hearing and hearing, such as the fees that must be paid to witnesses who have been subpoenaed (45 CFR 160.522), the form, filing, and services

of any documents (45 CFR 160.524), requirements related to motions, and how any stated period of time must be computed (45 CFR 160.526). The Enforcement Rule also authorizes the ALJ to impose sanctions on any party, attorney, or other person for failing to comply with an order or procedure, or other misconduct that interferes with the hearing. 45 CFR 160.530. Sanctions may include striking pleadings, dismissing the action, and ordering a party to pay attorneys' fees, among other things. *Id.*

Hearings

The Enforcement Rule contains detailed requirements governing hearings. See 45 CFR §§ 160.534-160.544. The respondent bears the burden regarding any affirmative defenses or challenges to the amount of a proposed CMP, including a claim that a proposed penalty should be reduced or waived. 45 CFR 160.534(b)(1). On the other hand, HHS bears the burden with respect to all other issues, including issues of liability and the existence of any aggravating factors in determining the amount of the proposed penalty. 45 CFR 160.534(b)(2). The standard that the burden will be judged by is a preponderance of the evidence. 45 CFR 160.534(b)(3). In meeting its burden, HHS is permitted to introduce the results of a statistical sampling study as evidence to establish the number of violations or other factors that were considered when calculating the amount of the CMP. 45 CFR 160.536. If this study is based upon an appropriate sampling and computed by valid statistical methods, then it will constitute prima facie evidence of the number of violations and other factors supporting the amount of the CMP. 45 CFR 160.536(a). The burden will then shift to the respondent to rebut the findings of the statistical study. 45 CFR 160.536(b).

Hearings must be open to the public unless otherwise ordered by the ALJ for good cause shown. 45 CFR 160.534(c).

The Enforcement Rule addresses admission of evidence (45 CFR 160.534(d) and 160.540), testimony of witnesses (45 CFR 160.538), and the record of the hearing (45 CFR 160.542). It also authorizes the ALJ to require the parties to file post-hearing briefs. 45 CFR 160.544. The parties are also authorized to file post-hearing briefs no later than sixty days from the date they receive the hearing transcript. *Id.*

The ALJ's Decision and Appeal Rights

The Enforcement Rule requires the ALJ to issue a decision within sixty days after the time for submission of post-hearing briefs and reply briefs, if permitted, has expired, and the decision must contain findings of fact and conclusions of law. 45 CFR 160.546(a) and (c). The ALJ has the authority to affirm, increase, or reduce CMPs imposed by HHS. 45 CFR 160.546(b). Unless the decision of the ALJ is appealed in a timely manner, the decision will be final and binding on the parties sixty days from the date of service of the ALJ's decision. 45 CFR 160.546(d).

Any party may appeal an ALJ decision. 45 CFR 160.548. Appeals are made to the HHS Departmental Appeals Board (Appeals Board). 45 CFR 160.548(a). To commence the process, a party must file a notice of appeal within thirty days of the date that the ALJ decision was served. *Id.* The Appeals Board has the authority to extend this thirty-day period by an additional thirty days. *Id.* A notice of appeal must be accompanied by a written brief, and any party may file a brief in opposition within thirty days of receiving the notice of appeal and the accompanying brief. 45 CFR 160.548(c). The Board may permit the parties to file reply briefs. *Id.* There is no right to appear personally before the Appeals Board. 45 CFR 160.548(d).

Decisions of the Appeals Board

The Appeals Board must serve the parties with its decision within sixty days after the time for submission of briefs and reply briefs has expired. 45 CFR 160.548(i). The Board must also provide a statement describing the right of any respondent who is penalized to seek judicial review. *Id.* The Appeals Board may decline to review the case or may affirm, increase, reduce, reverse, or remand any penalty determined by the ALJ. 45 CFR 160.548(g). The standard of review on a disputed issue of fact is whether the initial decision of the ALJ is supported by substantial evidence on the whole record. 45 CFR 160.548(h). The standard of review on a disputed issue of law is whether the decision is erroneous. *Id.*

The Board's decision becomes final sixty days after the date of service of the Board's decision, except with respect to a decision to remand to the ALJ or if reconsideration is requested. The Board will reconsider its decision only if it determines that the decision contains a clear error of fact or error of law. 45 CFR 160.548(j)(1), 45 CFR 160.548(j)(2). A party may file a motion for reconsideration with the Board before the date the decision becomes final. 45 CFR 160.548(j)(3). A motion for reconsideration must be accompanied by a written brief specifying any alleged error of fact or law and, if the party is relying on additional evidence, explaining why the evidence was not previously available. *Id.* Any party may file a brief in opposition within fifteen days of receiving the motion for reconsideration and the accompanying brief unless this time limit is extended by the Board for good cause shown. *Id.* Reply briefs are not permitted. *Id.*

The Board must rule on the motion for reconsideration not later than thirty days from the date the opposition brief is due. 45 CFR 160.548(j)(4). If the Board denies the motion, the decision becomes the final decision of the Secretary of HHS on the date of service of the ruling. *Id.* If the Board grants the motion, the Board will issue a reconsidered decision, after such procedures as the Board determines necessary to address the effect of any error. *Id.* The Board's decision on reconsideration becomes the final decision of the Secretary of HHS on the date of service of the decision, except with respect to a decision to remand to the ALJ. *Id.*

If a respondent wishes to petition for judicial review of a final decision, the petition must be filed within sixty days of the date on which the decision of the Board becomes the final decision of the Secretary. 45 CFR 160.548(k)(1). A copy of any petition for judicial review filed in any US Court of Appeals challenging the final decision of the Secretary must be sent by certified mail, return receipt requested, to the General Counsel of HHS. 45 CFR 160.548(k)(2). Pending judicial review, the respondent may file a request for stay of the effective date of any penalty with the ALJ. 45 CFR 160.550(a). The request must be accompanied by a copy of the notice of appeal filed with the federal court. *Id.* The filing of the request automatically stays the effective date of the penalty until such time as the ALJ rules upon the request. *Id.* The ALJ may not grant a respondent's

request for stay of any penalty unless the respondent posts a bond or provides other adequate security. 45 CFR 160.550(b). The ALJ must rule upon a respondent's request for stay within ten days of receipt. 45 CFR 160.550(c).

Internal Investigations

Follow a Complaint Handling and Investigation Policy

Clients should have a robust complaint and investigation handling policy and procedure that includes a checklist of the steps to follow in the event of any privacy-related complaint or government investigation. The Privacy Officer should be immediately notified of any such complaint or government investigation.

The Privacy Officer's first step will be to open an internal investigation of the issue. As part of the internal investigation, the Privacy Officer should interview employees or contractors involved in the issue and review relevant documents. Such documents will likely include applicable policies and procedures. The Privacy Officer should evaluate whether the policies and procedures are adequate in light of the incident at issue. In the event that an OCR investigation has been opened, the OCR will also likely request copies of such policies and procedures, as well as the result of the internal investigation.

The Enforcement Rule requires Covered Entities to maintain and submit records and reporting as requested by HHS, to cooperate with complaint investigations and compliance reviews, and to permit HHS and OCR access to its facilities, books, records, and other relevant information. 45 CFR 160.310. As a result, it will be important for the Privacy Officer to proactively identify any deficiencies and document them as part of the internal investigation report, as well as any changes that will be implemented to cure such deficiencies.

Sanctions

It will also be important for the Privacy Officer to determine whether any employees have violated the organization's privacy-related policies and

procedures. Such determination must be documented. In the event that an employee has violated HIPAA or the organization's policies and procedures, appropriate sanctions must be imposed and documented pursuant to the organization's discipline policies. If it is determined that a contractor has violated HIPAA, or the organization's policies and procedures to the extent applicable to the contractor, or the organization's agreement with the contractor, appropriate sanctions must also be imposed and the Privacy Officer must document that decision. If the contractor is a Business Associate or sub-contractor, then the Business Associate Agreement or Subcontractor Business Associate Agreement must be reviewed to determine contractual remedies. If the contractor provided services on-site and was treated as a member of the organization's workforce, then appropriate sanctions must be imposed and documented.

Analyze Issue, Involve other Departments

As part of the internal investigation, the Privacy Officer must determine whether the problem at issue was isolated or the result of a systemic issue. In the event of a systemic problem, the Privacy Officer may need to involve other individuals within the organization, such as the information technology (IT) department, legal department, or human resources (HR) department. In addition to changes in policies and procedures, an evaluation of the other systems and processes within the organization may be necessary. It is important to try to anticipate the systems and processes that the government may review as part of an investigation in order to identify issues and proactively address them.

Mitigation

In the event that the internal investigation was triggered by a privacy-related complaint from an individual, the organization's response to such complaint will be critical and may help prevent the complainant from submitting a complaint to OCR and triggering an investigation. As a result, it will be critical to evaluate any steps that can be taken to mitigate potential harm that may result from the activity that triggered the complaint. Such steps may include a simple apology to the complaining individual, if appropriate. Organizations may resist admitting that a privacy-related violation occurred. However, if the results of the internal investigation

reveal inappropriate conduct, proactively acknowledging that this occurred, indicating that steps will be taken to help prevent such conduct from occurring in the future, and an apology may help satisfy the complainant and resolve the issue early. Even if the complainant is not satisfied and complains to OCR, triggering an investigation, OCR may determine that the organization resolved the issue itself by taking such steps. It is important to note that OCR may require such steps be taken as a result of its investigation.

In the event that an internal investigation is triggered by an OCR investigation, the same concepts will apply. As noted in the above section, OCR will attempt to resolve the case through voluntary compliance, and if not possible, then through corrective action or a resolution agreement. It will be in the best interests of an organization to resolve issues proactively through voluntary compliance. It will also be important to avoid any charges that it acted with willful neglect in not identifying and correcting HIPAA violations.

No Intimidation or Retaliation

It is critical to any compliance effort that a policy is implemented and followed to prohibit any intimidation or retaliation against anyone, including employees and patients, or any other person for filing a complaint or testifying or assisting in an investigation or compliance review or other proceeding, or opposing any practice that the person in good faith believes violates HIPAA. 45 CFR 160.316.

Important Note

Each step is important because each is fundamental to identifying problems and proactively resolving them to mitigate the risk of an enforcement action, as well as to prevent future problems.

The Lawyer's Role

The lawyer's role will vary throughout the process. Often, the lawyer takes a "behind the scenes" role in the early stages of a privacy-related complaint or OCR investigation. The lawyer will work with the Privacy Officer and

the client to advise on the internal investigation and to evaluate the initial drafts documenting the internal investigation. Depending on this issue and the internal resources of the client, the lawyer may simply help evaluate risk, provide input to help finalize the documentation, and advise on mitigation strategies, while communications with the OCR will be handled by the Privacy Officer. The lawyer may take a more visible role if, for example, it is likely that the issue will not be resolved through voluntary compliance or if there is disagreement with the OCR's position.

If the results of the internal investigation reveal that a more extensive compliance audit is warranted, the lawyer who is acting as outside counsel may directly engage the consultant or other third party who will conduct the audit to preserve attorney-client privilege. The best way to avoid enforcement actions is to promote a strong culture of compliance. Steps to ensure a strong and robust compliance program include rigorous implementation of HIPAA Privacy and Security Policies, meaningful training of employees, recurring compliance audits, and plans for promptly and thoroughly responding to privacy or security incidents.

Prepare for Enforcement

One of the key actions to prepare for any enforcement proceeding is to conduct periodic assessments of both documentation and processes. The following describes each category of preparatory steps.

Documentation Review

The most critical component of a HIPAA compliance program is documentation. The first thing OCR will ask for in any complaint investigation or compliance review will be a copy of the Covered Entities' HIPAA policies and procedures and other documentation required by HIPAA, such as the Notice of Privacy Practices, authorization forms, accounting of disclosures logs, etc., to the extent relevant to the complaint investigation or compliance review. The quality and completeness of such documentation will form OCR's impression of the entity and its compliance efforts. As is typical when dealing with enforcement by any regulatory agency, if there is insufficient documentation to support compliance, then

the regulators will presume actions necessary to achieve compliance were not done, no matter what the Covered Entity says to the contrary.

Organizations often do not have the resources or do not wish to allocate resources for robust policies and procedures. Prior to the HITECH Act and change in the enforcement environment, this may have been a risk worth taking. However, in the new era of heightened enforcement, such strategy may ultimately cost the organization far more than it would have spent on robust documentation because OCR may determine the lack of policies and procedure rises to the level of willful neglect.

The next step is to regularly review HIPAA policies, procedures, and related documentation to ensure that they are current and adequately address any changes within the organization. Staff should be appropriately trained on HIPAA policies and procedures, and documentation evidencing such training efforts should be up-to-date.

Processes

In addition to having the appropriate policies, procedures, and other documentation in place, when preparing for enforcement proceedings, it is important to check that the processes to comply with HIPAA outlined in the policies and procedures are being followed and actually work. The best method to do so is through the audit process. It is likely that an organization will have an OCR compliance review audit, since such audits are mandated by the HITECH Act. As a result, it is excellent preparation for an organization to conduct its own audit.

Security Rule Audits

Audits can be done internally or through an outside third party, depending on the organization's resources. The HIPAA Security Rule requires an organization to perform an initial risk assessment, as well as a periodic assessment, which will essentially be the basis for the audit. 45 CFR §§ 164.3069a)(1)(i)(A) and 164.306(a)(8). In addition to auditing for workforce compliance with the processes set forth in the Security Policy and Procedures, the electronic systems must be checked for compliance with Security Rule safeguards. As a result, the audit team will need to be

comprised of individuals with the appropriate background, training, and skill sets.

Security Rule enforcement was recently criticized by the Federal Office of Inspector General, which conducted an audit of seven hospitals for information on areas targeted by the Inspector General as vulnerable and lacking compliance. See the report at <http://oig.hhs.gov/oas/reports/other/180930160.pdf>. The Office for Civil Rights and the predecessor Security Rules enforcement agency, CMS, have also provided guidance on areas of risk or Security Rule noncompliance. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf>, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf>.

Privacy Rule Audits

A Privacy Rule audit will be focused on process to ensure that policies and procedures are being followed and that there are no compliance gaps. The biggest area of risk is impermissible uses and disclosures of PHI and e-PHI. As a result, that is an important area of focus, especially in light of the new Breach Notification requirements.

Although HIPAA Privacy and Security compliance involves different issues and areas of expertise, they cannot each be reviewed in a silo because HIPAA Security supports the ability to comply with the HIPAA Privacy Rule. Moreover, security can help prevent impermissible uses and disclosures to help avoid triggering the Breach Notification Requirement. In addition, even if a breach occurs, use of encryption and other security measures in accordance with the OCR's Guidance can mean the breach is not reportable.

Privacy and Security Officers

Both the Privacy Rule and the Security Rule require Covered Entities to appoint a Privacy Officer and a Security Officer. As a result, it is critical to compliance that qualified individuals with appropriate knowledge of HIPAA, health information management practices, and NIST Standards are appointed to take those roles. Most organizations did have a Privacy and

Security Officer; however, prior to the HITECH Act, it was common that these two officers had little interaction with each other. With the HITECH Act and the advent of mandatory breach notification, as well as other new requirements related to e-PHI (e.g., new requirements governing access rights to e-PHI, new proposed rule on accounting of disclosures), it is clear that these two officers need to work closely together, both with the audit process and in general compliance efforts.

Lawyer's Role in Audits

The lawyer can assist in the audit process in a number of ways. First, if an audit will be conducted by an outside third party, the lawyer can engage the third party to maintain attorney-client privilege. The lawyer can also help further educate auditors on areas of risk and help review audit results and analyze risk.

A Note about Insurance

In light of the increased potential for liability under HIPAA, the lawyer should consider recommending that his or her clients purchase insurance to cover HIPAA risks. Although such policies will not cover criminal fines or penalties, coverage should be obtained for costs associated with responding to security breaches. The lawyer should consider recommending coverage that would also cover defense of actions brought for allegations of HIPAA violations and imposition of civil penalties.

Conclusion

HIPAA enforcement will unquestionably increase over the next few years. As discussed above, the OCR will start conducting compliance audits soon. State attorneys general will also likely bring more HIPAA suits after receiving training. The DOJ has also increased its HIPAA enforcement by its recent criminal indictments. Further, since Covered Entities have to report security breaches of unsecured PHI to individuals, the OCR, and potentially the media, it is likely that more penalties will be imposed on Covered Entities and Business Associates, and more state privacy suits likely will be filed. Further, if a breach occurs of more than 500 individuals, the OCR has indicated that it will conduct a compliance audit of the

Covered Entity who reported the breach, which will likely result in increased penalties. Finally, Business Associates will also need to start ramping up their HIPAA compliance efforts because they are also directly liable for penalties under HIPAA.

Key Takeaways

- Prepare for an increase in HIPAA-related audits and penalties.
- Understand current HIPAA and state privacy law requirements, and stay on top of updates.
- Familiarize yourself with the HIPAA complaint process, how to investigate complaints, and how to respond to complaints.
- Review your organization's HIPAA privacy and security policies and procedures to ensure they comply with applicable law in preparation for an audit.
- Periodically conduct risk assessments, as required by the HIPAA Security Rule.
- Secure PHI by encrypting data and destroying PHI in accordance with HHS Guidance and NIST Standards.
- Be aware of the potential civil and criminal penalties associated with HIPAA and state law privacy violations.

***Lisa J. Acevedo** is a partner in the Health Law Group at Quarles & Brady LLP. She provides regulatory and transactional advice and general counsel to clients representing virtually all aspects of health care. She counsels clients on compliance with statutes and regulations affecting companies doing business in the health care industry, including the anti-kickback statute, Stark, the Food, Drug and Cosmetic Act, and implementing regulations, including the Prescription Drug Marketing Act. Ms. Acevedo counsels clients on compliance with other federal and state privacy and security laws, regulations, and standards governing personally identifiable information. She has assisted clients through security breaches and the notification process, both at the federal and state levels.*

Ms. Acevedo was previously corporate counsel within Baxter International, where she led the creation and implementation of the company's global privacy program.

Martindale-Hubbell CV Peer-Review Rated, Ms. Acevedo has written several articles and delivered a number of speeches on privacy and security matters, including HIPAA compliance, as well as health care fraud and abuse, Stark, tax-exempt issues and FDA issues. She has been an adjunct instructor of health law at Benedictine University in its Master's in Public Health graduate program.

A member of the American Bar Association, Ms. Acevedo also holds membership in the Hispanic Lawyers Association of Illinois and the American Health Lawyers Association.

Ms. Acevedo received her JD, with honors, from DePaul University College of Law, where she served as the article and note editor of the DePaul Business Law Journal. She earned her BS from Loyola University. She is admitted to practice in the State of Illinois.

Jennifer L. Rathburn *is a partner in the Health Law Group of Quarles & Brady LLP. She provides regulatory and transactional advice and general counsel to health care providers, health plans, employers, and other companies doing business in the health care industry.*

Ms. Rathburn advises clients in the areas of general health care law, including regulatory compliance issues, reimbursement, federal privacy and security laws, state laws governing medical record confidentiality, privacy and security issues regarding electronic medical records and data bases, and privacy and security breach investigations.

Selected for inclusion in Wisconsin Super Lawyers—Rising Stars for 2006, 2007, and 2008 in health care, Ms. Rathburn holds membership in the American Bar Association (member, Health Law Section), the American Health Lawyers Association, and the American Health Information Management Association. She serves on the board of directors of the Curative Care Network and on the Behavioral Health Advisory Committee of Aurora Psychiatric Hospital Inc.

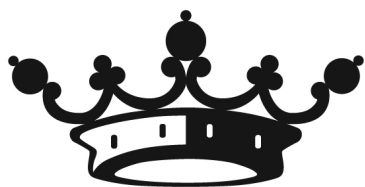
Ms. Rathburn earned her JD, magna cum laude, at St. Louis University School of Law, where she served on the St. Louis University Law Journal and was a member of the Health Law Society. She received a BA in psychology, magna cum laude, from the University of Kentucky, where she was a member of Phi Beta Kappa. She is admitted to practice in Wisconsin and Illinois.



ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.

Each chapter in the *Inside the Minds* series offers thought leadership and expert analysis on an industry, profession, or topic, providing a future-oriented perspective and proven strategies for success. Each author has been selected based on their experience and C-Level standing within the business and legal communities. *Inside the Minds* was conceived to give a first-hand look into the leading minds of top business executives and lawyers worldwide, presenting an unprecedented collection of views on various industries and professions.



ASPATORE