MEADE & ROACH LLP
ATTORNEYS AT LAW

Client Advisory: HIPAA

February 2006

HHS Publishes Final HIPAA Enforcement Rule and Sets New Tone for HIPAA Investigations: Covered Entities Should Check Health of HIPAA Compliance Programs & Do HIPAA Audits Before March 16

A New HIPAA Era Begins

Up until now, no covered entity has been fined in the course of more than 16,000 HIPAA investigations undertaken by the Federal government since the HIPAA Privacy Rule's compliance date in April 2003 – though a small portion of egregious violations have been referred to the Department of Justice for criminal prosecution. For the most part, as long as a covered entity cooperated with OCR or CMS during a privacy or security investigation, the covered entity was reasonably sure that the matter could be worked through without pain of penalty. The days of no penalties are over and the healthcare industry is likely to see its first fines later this year.

On February 16, 2006, the U.S. Department of Health & Human Services ("HHS") published the final HIPAA Enforcement Rule in the Federal Register. 71 Fed. Reg. 8390. The Enforcement Rule applies to regulations promulgated under the Administrative Simplification Provisions of HIPAA, including the Privacy Rule, the Security Rule and the Transactions Rule, collectively now referred to by HHS as the "HIPAA Rules." The Enforcement Rule establishes uniform processes that OCR (for privacy) and CMS (for all non-privacy HIPAA Rules) will follow when investigating noncompliance with the HIPAA Rules.

The new regulations also set out the bases for imposing civil money penalties, resolving noncompliance by "informal means," the process for allowing a covered entity to offer an affirmative defense, and an array of rules allowing for appeal and hearing of a civil money penalty determination.

The Enforcement Rule's investigation procedures encourage quick, voluntary compliance as a means to avoid penalties, but mandates penalties if the covered entity cannot set out mitigating factors or an affirmative defense. The official commentary clarifies that once HHS determines that a violation has occurred and no affirmative defense exists, then HHS believes the HIPAA statute requires it to impose a civil money penalty.

Effective Date

The Effective Date for the Enforcement Rule is March 16, 2006. Since these rules are not considered implementation regulations under HIPAA, the usual two year compliance period does not apply and covered entities have been given one month to prepare for the effective date of the Enforcement Rule. Covered entities have until March 16 to get their HIPAA house in order before the new enforcement era begins.

The New Investigation Process

The Enforcement Rule sets out a new process that HHS will follow when investigating HIPAA noncompliance. After conducting an investigation of the alleged noncompliance and determining that a violation occurred, HHS will propose resolution of the violation by "informal means." The regulations state that informal means "may include demonstrated compliance or a completed corrective action plan or other agreement." If a violation is resolved by informal means, then no penalty will be imposed.

Resolution by informal means will likely take many forms, including suggested corrective actions by HHS, but the most important form will be a recognition by HHS that the covered entity voluntarily corrected the noncompliance within 30 days of learning of the violation. As discussed below, this makes having an effective HIPAA compliance program a critical element for a covered entity to avoid civil money penalties.

If the violation cannot be resolved by informal means, then HHS will notify the covered entity in writing that the matter is not sufficiently resolved or resolvable by informal means and provide the covered entity "an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration…." The covered entity will have 30 days to submit its response.

An affirmative defense can include the covered entity demonstrating that it "did not have knowledge of the violation…and, by exercising reasonable diligence, would not have known that the violation occurred." HHS also allows an alternative affirmative defense that the violation is due to "reasonable cause and not willful neglect." The regulations define reasonable cause as circumstances that made it "unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply…."

Under either argument, the covered entity must also show that the noncompliance was corrected within 30 days of either when the covered entity knew of the violation or would have known if the covered entity had exercised "reasonable diligence." A solid and effective HIPAA compliance program will be the most important factor in avoiding penalties. Effective compliance structures to train workforce, respond to noncompliance quickly, audit corrective actions and audit generally to detect noncompliance or confirm compliance is the best protection against the Enforcement Rules' process for imposing civil money penalties.

Other Clarifications

The commentary to the Enforcement Rule provides important clarifications to a variety of lingering HIPAA ambiguities. Among them include:

- **A HIPAA violation can be an act or omission.** HHS strongly emphasizes that noncompliance can come in the form of both inappropriate activities (e.g, using or disclosing PHI in ways not allowed by the Privacy Rule) or *omissions* of HIPAA obligations (e.g., not distributing Notices of Privacy Practices or not establishing security safeguards).

- **Approach to addressable security implementation specifications must be in writing.** The Security Rule allows covered entities to utilize alternative security approaches to addressable implementation specifications if the addressable specification is not "reasonable and appropriate." If the addressable implementation specification is reasonable and appropriate, then the covered entity is required to implement the addressable specification. The Enforcement Rule commentary strongly asserts that when the addressable specification is not reasonable and appropriate, then "the covered entity must document why it would not be reasonable and appropriate to implement the implementation specification and implement 'an equivalent alternative measure if reasonable and appropriate'…." Creating this written documentation "is a requirement, and implementing an alternative measure is also a requirement, if doing so is reasonable and appropriate in the covered entity's circumstances." Furthermore, the com-

mentary clarifies that "failure to take either required action would, accordingly, constitute a violation."

- **HHS may do not-for-cause HIPAA audits.** The regulations specifically provide HHS the ability to perform "compliance reviews" at HHS's discretion. The commentary states that a complaint-only based system of enforcement is not sufficient to ensure industry compliance.

What Should Covered Entities Do?

Covered entities should spend the next month shoring up their HIPAA compliance programs to ensure they enter the new HIPAA enforcement era in as strong a position as possible. Accordingly, we suggest that covered entities undertake three actions as quickly as possible:

1. Conduct Gap Analysis of HIPAA Compliance Program Structure. The best approach to avoiding penalties is for a covered entity to have an effective HIPAA compliance program that implements not only the administrative structures required by the HIPAA rules, but also the basic elements of a compliance program. Covered entities should undertake a structural analysis of its HIPAA compliance program to ensure that all administrative aspects of the HIPAA compliance program are operating effectively. This analysis should be documented.

2. Begin Regular Privacy & Security Audits. One of the key elements of an effective compliance program is on-going auditing and monitoring. This is no different for HIPAA. Conducting regular privacy and security audits will help identify HIPAA noncompliance or demonstrate that the covered entity undertook reasonable diligence to identify noncompliance and did not have knowledge of noncompliance. HIPAA audits should be documented in writing and formalized. *If a covered entity has not performed a privacy or security audit since establishing its HIPAA program, then it is highly recommended that the covered entity perform a HIPAA audit before March 16, 2006.*

3. Review Security Addressable Implementation Specification Documentation. HHS strongly emphasized the need for covered entities to have documentation in place of its approach to the Security Rule's addressable implementation specifications. The addressable specifications have been one of the healthcare industry's most difficult challenges in complying with the HIPAA Security Rule. We suggest that covered entities review all addressable implementation specifications and develop a clear free-standing document that articulates the covered entity's approach to each of the addressable implementation specifications.

Contact Information

If you would like more information about the final HIPAA Enforcement Rule or would like to learn more about Meade & Roach's HIPAA compliance services, please contact **Michael Roach at (312) 255-1773** or **Ryan Meade at (312) 498-7004**. Meade & Roach, LLP offers a variety of HIPAA compliance services, including structural gap analyses and HIPAA audit assistance.

Meade & Roach, LLP is a law firm that focuses its practice on healthcare regulatory issues, concentrating on HIPAA, Medicare compliance, clinical trial research compliance, and other corporate compliance matters affecting the healthcare industry. More information about Meade & Roach, LLP, and its affiliated consulting firm, Meade Roach Consulting, LLP, is available on the Internet at **www.MeadeRoach.com**.