GSB Healthcare Legal Update

HIPAA: Proposed Regulations to the HIPAA Privacy, Security and Enforcement Rules Under HITECH

Notice of Proposed Rulemaking issued July 14, 2010

Changes and Modifications to the Enforcement Rules and Enforcement Provisions

Introduction

The Health Information Technology for Economic and Clinical Health Act ("HITECH Act") mandated the U. S. Department of Health and Human Services ("HHS") issue regulations modifying the HIPAA Privacy, Security, and Enforcement Rules. On July 14, 2010, HHS formally issued its Notice of Proposed Rulemaking ("NPRM") to comply with HITECH.

In addition to bringing itself into compliance with HITECH, HHS took this opportunity to issue additional proposed changes and modifications to HIPAA. HHS explains in the commentary to the NPRM:

> While passage of the HITECH Act necessitates much of the rulemaking in the [NPRM], it does not account for all of the proposed changes to the HIPAA Privacy, Security, and Enforcement Rules encompassed in this rulemaking. [HHS] is taking this opportunity to improve the workability and effectiveness of all three sets of HIPAA Rules. . . . [In the last eight] years, HHS has accumulated a wealth of experience with these rules, both from public contact in various forums and through the process of enforcing the rules. . . . Accordingly, we propose a number of modifications that we believe will eliminate ambiguities in the rules and/or make them more workable and effective. Further, we propose a few modifications to conform the HIPAA Privacy Rule to provisions in the Patient Safety and Quality Improvement Act of 2005.

The purpose of this memorandum is to present and construe the proposed changes to the HIPAA Enforcement Rules. Subsequent additions to this memorandum will discuss the proposed changes to the other HIPAA Rules.

Levels of Culpability

HHS issued an interim final rule ("IFR") on October 30, 2009, revising the Enforcement Rule to incorporate the provisions required by the HITECH Act. The HITECH Act created four

categories of violations that reflect increasing levels of culpability with corresponding tiers of civil money penalties ("CMP"). The new penalty provisions apply to violations occurring on or after February 18, 2009.

Tier A—Violation Without Knowledge

The least stringent level of CMPs applies to violations where it is established that the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision of HIPAA. The CMPs for this level of violation are not less than $100 or more than $50,000 for each violation.

The "knowledge" involved here must be knowledge that a violation has occurred, not just knowledge of the facts surrounding the violation. Further, a covered entity or business associate cannot assert an affirmative defense associated with its "lack of knowledge" is that lack of knowledge has resulted from its failure to inform itself about compliance obligations or to investigate received complaints or other information indicating likely noncompliance.

By way of an example of a Tier A violation, HHS poses the following hypothetical:

> A covered health care provider with a direct treatment relationship with an individual patient failed to provide the patient a complete notice of privacy practices in compliance with § 164.520(c). HHS's investigation reveals that the covered entity has a compliant notice of privacy practices, policies and procedures for provision of the notice, and appropriate training of its workforce regarding the notice and its distribution. The violation resulted from a printing error that failed to print two pages of the notice of privacy practices. The printing error affected a small number of the covered entity's supply of notices and was an isolated failure to provide an individual with the covered entity's notice of privacy practices.

Even though the hypothetical fails to show how the covered entity had "knowledge that a violation had occurred," HHS appears to presume such knowledge and then points out that the covered entity acted with reasonable diligence because:

- The covered entity had compliant policies and procedures in place; and
- There appeared to be good faith efforts by the covered entity to implement the Privacy Rule requirements.

he hypothetical underscores the importance of having compliant policies and procedures in place.

Tier B—Reasonable Cause And No Willful Neglect

The next level of CMPs applies to a violation where it is established that the violation was due to reasonable cause and not due to willful neglect. The CMPs for this level of violation are not less that $1,000 or more than $50,000 per violation.

The NPRM proposes that this "Reasonable Cause" level of culpability apply to the following:

- Situations where circumstances would make it unreasonable for the covered entity or business associate, despite the exercise of ordinary business care and prudence, to comply with the provisions violated;
- Situations where a covered entity or a business associate has knowledge of a violation but lacks the conscious intent or reckless indifference associated with the willful neglect category (tier) of violations.

Therefore, the NPRM proposes to replace the current definition of "reasonable cause" with the following:

> 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.

The commentary to the NPRM poses the following example of how this definition will be applied if adopted:

> A covered entity received an individual's request for access but did not respond within the time periods provided for in § 164.524(b)(2). HHS's investigation reveals that the covered entity had compliant access policies and procedures in place, but that it had received an unusually high volume of requests for access within the time period in question. While the covered entity had responded to the majority of access requests received in that time period in a timely manner, it had failed to respond in a timely manner to several requests for access. The covered entity did respond in a timely manner to all requests for access it received subsequent to the time period in which the violations occurred.

Analyzing the above hypothetical HHS states that there was a violation and that the covered entity had knowledge of the violations. However, the facts indicate that this would be a Tier B—Reasonable Cause And No Willful Neglect violation because the circumstances made it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the provisions violated. HHS reasoned that willful neglect could not be shown in the above example because:

- The covered entity showed good faith by having compliant policies and procedures in place on responding to an individual's request for access to records;
- The covered entity responded to the majority of access requests in a timely manner;

- The covered entity responded to all access requests in a timely manner subsequent to the time period in which the violations occurred.

HHS noted that if the failure to respond to the access requests had occurred over a longer period of time and the covered entity did not attempt to address the backlog or communicate with the affected individuals, in writing, regarding the reasons for the delay, a determination of willful neglect could have been made.

This hypothetical also emphasizes the importance of having compliant policies and procedures in place.

Tier C—Willful Neglect With Timely Correction

The two highest levels of CMPs require a showing of willful neglect. The next to highest level applies to a violation where it is established that the violation was due to willful neglect but was timely corrected. The CMPs for this level of violation are not less than $10,000 or more than $50,000 for each violation.

"Willful neglect" is defined to mean the "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." The term not only presumes actual or constructive knowledge on the part of the covered entity that a violation is virtually certain to occur but also encompasses a conscious intent or degree of recklessness with regard to its compliance obligations.

The "willful neglect" definition also applies to Tier D penalties. The distinction between Tier C and Tier D penalties is that Tier C applies where the covered entity or business associate timely corrects the violation and Tier D applies where there has not been a timely correction. As noted below, the concept of "corrected" may apply even if the violation is not fully undone. The HHS hypothetical is discussed below under the Tier D analysis.

Tier D—Willful Neglect and No Timely Correction

The highest level of CMPs applies to a violation where it is established that the violation was due to willful neglect and there was no timely correction. The CMPs for this level of violation, the highest, are not less than $50,000 for each violation.

In order to distinguish the differences between situations where Tier C and Tier D penalties will be imposed HHS provided the following hypothetical for analysis:

> A covered entity disposed of several hard drives containing electronic protected health information in an unsecured dumpster, in violation of § 164.530(c) and § 164.310(d)(2)(i). HHS's investigation reveals that the covered entity had failed to implement any policies and procedures to reasonably and appropriately safeguard protected health information during the disposal process.

The violations seem quite clear here. The facts show that the covered entity knew or should have known that it would be a violation to throw unsecured electronic protected health information in an unsecured dumpster. Following its theme of underscoring the importance of having compliant policies and procedures in place, HHS emphasizes that this lack of compliant policies and procedures coupled with a failure to respond as required by § 164.400 et seq. "demonstrates either a conscious intent or reckless disregard with respect to their compliance obligations.

In drawing the distinction between impositions of Tier C and Tier D penalties HHS notes that while a covered entity's or business associate's correction of a willful neglect violation will not bar the imposition of a CMP, such correction may foreclose HHS's authority to impose Tier D penalties. While no one wants to be subject to any CMPs, given a choice between Tier C penalties and Tier D penalties, application of Tier C instead of Tier D could save a covered entity tens of thousands of dollars in CMPs.

HHS also notes that not all violations can be "corrected" in terms of being fully undone or remediated. Therefore, HHS has been using a broad interpretation of "corrected." For example, in the event a covered entity's or business associate's inadequate safeguards policies and procedures result in an impermissible disclosure, the disclosure violation itself might not be able to be fully undone or corrected. The "safeguards" violation, however, could be "corrected" in the sense that the noncompliant policies and procedures could be brought into compliance. HHS also notes that for these situations "corrective action will always be required of a covered entity or business associate.

Maximum Cumulative Penalty

A CMP for violations of the same requirements or prohibition under any of the above categories (tiers) may not exceed $1,500,000 in a calendar year.

Affirmative Defenses

The IFR also revised certain affirmative defenses for violations occurring on or after February 18, 2009, to remove a covered entity's lack of knowledge as an affirmative defense and to provide an affirmative defense when violations not due to willful neglect are corrected within 30 days.

Conclusion

HHS through its commentary to the NPRM issued on July 14, 2010, has made clear that it plans to step up enforcement efforts and plans to actively enforce its new four-tier civil money penalties. Further, HHS, through the use of hypothetical facts, has made clear that it intends to pursue for CMPs what many might consider to be very minor or technical violations. At the very least, all covered entities and business associates should take to time to make sure their policies and procedures are fully compliant.