HHS Proposed Major Changes to HIPAA Privacy, Security and Enforcement Rules

July 12, 2010

SECURITY & PRIVACY ALERT - JULY 12, 2010

written by Colin J. Zick, Maia M. Larsson

On July 8, 2010, the Department of Health and Human Services ("HHS") issued a notice of proposed rulemaking ("NPRM" or "proposed rule")[1] modifying the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy, Security, and Enforcement Rules[2] pursuant to the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which was enacted February 17, 2009 as part of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5.

The NPRM will be published in the Federal Register on July 14. Stakeholders will have 60 days from the date of publication to submit comments on the proposed rule to HHS.

Overview

The proposed modifications in this NPRM are intended to implement recent amendments made under the HITECH Act and to "improve the workability and effectiveness" of the HIPAA Rules. In the NPRM, HHS describes section-by-section how the proposed regulatory changes would implement provisions of the HITECH Act. In addition, HHS has proposed technical corrections and other modifications to enhance the effectiveness of the Rules.[3]

In summary, the proposed changes include:

- Extending to business associates many of the requirements in the Privacy and Security Rules;
- Establishing new limitations on the use and disclosure of protected health information for marketing and fundraising purposes;
- Restricting the disclosure of protected health information ("PHI") to health plans;
- Expanding individuals' rights to access their information; and
- Expanding HIPAA's enforcement of privacy and security provisions.

Proposed Amendments to the Privacy Rule

With specific regard to "business associates," HHS's proposed rules confirm the extension of HIPAA privacy and security rules to them (essentially making "business associates" into "covered entities.")

HHS also seeks to modify the definition of "business associate" to conform with its statutory definition and to provide clarification on circumstances that would give rise to a business associate relationship. For example, HHS proposes to add patient safety activities to the list of functions and activities that would give rise to a business associate relationship if a person undertook those activities on behalf of a covered entity. *Id.* at 19. In addition, several types of organizations that did not exist when the HIPAA regulations were finalized a decade ago, such as a Health Information Exchange Organization, E-prescribing Gateway, or Regional Health Information Organization, will be treated as business associates. *Id.* at 20.

In an expansion of HIPAA beyond even the provisions of HITECH, HHS proposes to add that subcontractors ("those persons that perform functions for or provide services to a business associate") to the definition of a business associate. *Id.* at 22. This has the potential to extent HIPAA to many entities not covered previously.

HHS discusses the new HITECH Act requirements affecting the Privacy Rule and proposes further regulatory changes including changes related to the definition of "marketing" and use and disclosure rules for PHI applicable to business associates. *See id.* at 64-82. To address the concern by covered entities and business associates regarding administrative burdens and costs related to implementing revised contracts around new proposed regulations, HHS proposes to allow covered entities and business associates (and their subcontractors) to continue operating under their existing contracts for up to one year beyond the compliance date of the revisions to the Rules. *See id.* at 87-88.

Regarding the use and disclosure of PHI where valid authorization is required, the proposed rule would add an addition circumstance to the existing two circumstances in current regulations where such authorization is necessary. Currently, authorization is required for (1) most uses and disclosures of psychotherapy notes; and (2) uses and disclosures for marketing. In accordance with the third circumstance added by the HITECH Act – the sale of PHI – HHS proposes to add a new section to the regulations that would require a covered entity (or business associate) to obtain authorization for disclosure of PHI that is in exchange for director or indirect remuneration, unless a specified exception applies. *See id.* at 91-99.

Proposed Amendments to the Security Rule

HHS proposes a number of changes to the Security Rule including technical modifications as well as modifications to references to business associates, administrative safeguards, and organizational requirements. *See id.* at 56-64.

Effective Date and Compliance Period

Although most of the provisions of the HITECH Act already became effective February 18, 2010, HHS recognized that it will be difficult for covered entities and business associates to comply with the statutory provisions until after HHS has finalized its changes to the HIPAA Rules. As such, HHS intends to provide covered entities and business

associates with 180 days beyond the effective date of the final rule to come into compliance with "most of the rule's provisions." *Id.* at 13. This proposed 180-day compliance period, however, will not apply to the HIPAA Enforcement Rule "because such provisions are not standards or implementation specifications," and thus, these provisions will be in effect and apply at the time the final rule becomes effective or as otherwise provided. *Id.* at 15.

---

[1] HHS "Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act" (July 8, 2010) Display copy, available here [hereafter, "HHS NPRM"].

[2] Note: "Privacy Rule" refers to the Standards for Privacy of Individually Identifiable Health Information; the "Security Rule" refers to the Security Standards for the Protection of Electronic Protected Health Information; and the "Enforcement Rule" refers to Compliance and Investigations, Imposition of Civil Money Penalties, and Procedures for Healings, issued under HIPAA.

[3] Several sections of the HITECH are not discussed in detail in these regulations either because they have been the subject of previous rulemakings (e.g., breach notification), or will be the subject of future rulemakings (e.g., accounting for disclosures requirement, and the penalty distribution methodology requirement.)