Finally! HHS Issues Proposed Rule Implementing Changes to the HIPAA Privacy, Security and Enforcement Rules under HITECH

BY ALDEN BIANCHI, STEPHEN R. BENTFIELD, AND DIANNE J. BOURQUE

The U.S. Department of Health and Human Services (HHS) released long-awaited proposed regulations (the “proposed regulations”) implementing key provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Congress enacted the HITECH Act as part of the American Reinvestment and Recovery Act of 2009, codifying a host of significant changes to the HIPAA privacy, security, and enforcement rules. In addition HHS, through the proposed regulations, made some minor, technical changes to HIPAA. Although the February 17, 2010 effective date for many HITECH Act provisions has passed, the proposed regulations provide specific information on when HHS expects covered entities and business associates to comply with these obligations, and on when covered entities and business associates alike can expect the HHS Office of Civil Rights to begin enforcement efforts. Additional details about important compliance deadlines appear below. (Click here to access a copy of the proposed regulations.)

The purpose of this advisory is to provide an overview of the proposed regulations. When finalized, the proposed regulations will, by their nature, affect covered entities, business associates, and others in vastly different ways. The concerns of a large, integrated health care delivery system, for example, will differ radically from those of a state-licensed insurance carrier that issues group health coverage. Similarly, employer-sponsored group health plans, and their brokers, consultants and other service providers will face an entirely different set of challenges. We will, therefore, separately publish more detailed client advisories addressing the key features of the proposed regulations from the perspective of providers, carriers, group health plans, and other service providers.

Background

HIPAA’s administrative simplification provisions1 established requirements governing the electronic transmission, privacy, and security of “protected health...
At Congress’ direction, HHS subsequently developed a robust regulatory scheme that focused on privacy and security standards, together with an accompanying enforcement mechanism. Congress significantly amended this regulatory scheme with passage of the HITECH Act. Specifically, HITECH:

- Applied certain HIPAA privacy and all of the HIPAA security standards to business associates;
- Added new breach notification requirements that govern covered entities and business associates, and a parallel set of requirements governing “personal health record” (PHR) vendors;
- Clarified and narrowed HIPAA’s “minimum necessary” standard;
- Prohibited the sale of PHI without the individual’s authorization;
- Restricted the marketing of PHI for fundraising purposes;
- Adopted new enforcement rules and increased penalties for violation of the HIPAA privacy and security rules; and
-Granted individuals greater to access electronic medical records and the right to restrict the disclosure of certain information.

The proposed regulations do not address all of the HITECH changes. (HHS previously issued an interim final rule implementing the HITECH Act’s provisions relating to enforcement and breach notification, which are currently in effect.) Rather, the scope of these proposed regulations is limited to the following items:

- Expansion of individuals’ rights to access their information and to restrict certain of disclosures of PHI;
- Application of certain of the HIPAA privacy, security, and enforcement rules to business associates;
- Limitations on the use and disclosure of PHI for marketing and fundraising communications; and
- The prohibition on the sale of PHI without patient authorization.

**Highlights of the Proposed Regulations**

The following is a brief summary of the major components of the proposed regulations.

**Expanded Right of Access**

HIPAA grants individuals a right to access or receive a copy of their PHI. HITECH expands this right and requires covered entities that maintain PHI in an electronic health record (EHR) to provide an individual with a copy of his or her PHI in electronic format or to transmit an electronic copy to the individual's designee upon request. To apply the right of access more uniformly, the proposed regulations require covered entities to make PHI in any format available in some type of electronic copy—in PDF format for example—even if it is not held in an EHR. The proposed regulations permit covered entities to work with individuals to identify an agreeable and technically feasibly means of
electronic transmission if the information is held in a form other than an EHR.

The proposed regulations also require a covered entity to transmit an electronic copy of the PHI to another person if the individual so requests in a clear, conspicuous, and specific manner. Again, the obligation to transmit in accordance with an individual’s request applies regardless of whether the PHI was originally held in an EHR. The rule defines “clear, conspicuous and specific manner” as a writing, signed by the individual, that clearly identifies the designated recipient and where to send the PHI.

**Expansion of Privacy and Security Rules to Business Associates**

Prior to the HITECH Act, HIPAA did not directly regulate business associates. The law required covered entities to enter into agreements with business associates that included business associate covenants, but the failure to enter into such agreements did not subject the business associate to any penalty or sanction. The HITECH Act makes a handful of important, substantive changes in this regard by:

- Applying the substantive provisions of the HIPAA security rule to business associates and making business associates liable for civil and criminal penalties for the failure to comply with these provisions;
- Making business associates civilly and criminally liable under the HIPAA privacy rule for any use and disclosure of PHI that does not comply with the terms of a business associate agreement;
- Subjecting business associates to the HITECH requirements enumerated above (e.g., breach notification rules, individual access to PHI, limitations on sale and marketing of PHI) and requiring business associate agreements to address these obligations; and
- Expanding the definition of “business associate” to include certain types of organizations (e.g., health information exchanges, e-prescribing gateways, and Regional Health Information Organizations) that provide data transmission of PHI to covered entities or business associates and that require routine access to PHI.

The proposed definition of “business associate” generally conforms to the requirements of the HITECH Act. It also clarifies that “Patient Safety Organizations” are deemed to be business associates for purposes of the privacy rule. In addition, HHS proposed to extend HIPAA’s privacy, security, and enforcement standards to subcontractors of business associates that create, receive, maintain, or transmit PHI on behalf of the business associate. HHS is therefore proposing to expand the number of organizations subject to HIPAA’s privacy and security rules, and enforcement actions.

From a HIPAA security standpoint, the inclusion of business associate subcontractors has two notable effects. First, subcontractors would be required to implement “reasonable and appropriate” security safeguards similar to those required of business associates to prevent improper use and disclosure of PHI, and to protect against breaches of unsecured PHI. Second, the business associate would effectively operate as a covered entity when working with subcontractors by, for example, obtaining required satisfactory assurances.
from subcontractors and entering into business associate agreements with them.

Although the covered entity retains ultimate responsibility for protecting PHI, HHS clarified in the preamble to the proposed regulations that it does not intend the modification to require covered entities to directly contract with the business associate subcontractor. Rather, the “obligation is to remain with the business associate who contracts with the subcontractor.”

**Restrictions on Marketing Uses and Disclosures of PHI**

HIPAA generally prohibits the use and disclosure of PHI for marketing purposes without an individual’s authorization; however, certain health-related communications are exempt from the definition of “marketing” and are thus permitted without authorization.

HITECH further restricts the use and disclosure of PHI for marketing and prohibits even health-related communications if the covered entity making the communication has received direct or indirect payment from the organization whose product or service is being described. Note that the prohibition only applies if payment is provided in exchange for the communication and only if payment is from the entity whose product or service is being described. For example, a charitable foundation may fund health-related communications about a state-of-the-art drug or medical device without violating the prohibition because the entity whose product or service is being described is not providing the funding for the communication.

To implement HITECH’s new marketing restrictions, HHS is proposing that covered entities give notice to patients and an opportunity to opt out of receiving subsidized communications. The proposed regulation requires covered entities to include a statement in their Notices of Privacy Practices when subsidized communications are a possibility and to provide opt-out information.

HIPAA’s original marketing provisions are complex and can be difficult to apply in practice. HITECH and the proposed regulations create additional layers of complexity and should be carefully considered in advance of any marketing-type communication involving the use or disclosure of PHI.

**Prohibition on the Sale of PHI**

HITECH prohibits the sale of PHI without an individual’s valid authorization. Under the proposed regulations, the authorization must make clear that the covered entity will be paid for its disclosure of PHI and must specify whether the PHI may be further sold by the recipient of the PHI. The proposed regulations list a number of exceptions to the prohibition, including disclosures for public health activities, research, treatment of the individual, or the disclosure of PHI in connection with the sale, merger, or other transaction involving a covered entity.

Covered entities should review existing authorization forms and consider whether revisions may be necessary in light of the proposed regulations.
Effective Dates

The HITECH Act specifies various effective dates that apply to different provisions. For example, the HITECH Act penalty provisions took effect on enactment while the breach notification rules were effective 180 days after enactment. Many of the HITECH Act's provisions that are the subject of the proposed regulations were slated to take effect one year after enactment, or February 18, 2010. Because this date has already passed, HHS proposes to adopt a later regulatory effective date, which is 180 days after the date HHS publishes the final rule in the Federal Register. (While this extension is welcome relief, it would have been better if HHS had made the announcement before February 18, 2010.) Parties to existing business associate agreements are afforded additional relief under the proposed regulations, having up to a full year following the publication of the final rule to amend or replace existing agreements (this relief is only available where there is a business associate agreement in place that conforms to the requirements of prior law.).

Next Steps

Although HHS delayed the effective dates for many of the proposed regulations, we strongly caution against interpreting this delay as permission to do nothing. HHS intends this grace period to provide covered entities, business associates, and subcontractors sufficient time to absorb and implement these new requirements. The HITECH Act’s message about enforcement is loud and clear: doing nothing can cost you dearly. Covered entities, business associates, and their subcontractors in particular, must begin to take good faith steps toward compliance.

Endnotes