



HITECH Regulations Update Still a Work in Progress

By Anthony J. Munns, CISA, FBCS, CITP

You may recall that we are waiting for the updated HITECH rule modifications – HHS in December told us they would be out by the end of March 2011. Well, guess what, we are still waiting.

Susan McAndrew, Deputy Director of Health Information Privacy at HHS OCR, said Tuesday May 10, 2011 at the Safeguarding Health Information conference OCR hosted with the National Institute of Standards and Technology (NIST) in Washington, that the final rules implementing the HITECH Act are to be released within months, if not weeks...

OCR is intending to issue multiple outstanding regulations at one time so that organizations can remediate compliance at one time, she explained. The regulations will include:

- HITECH Act-mandated modifications to the HIPAA privacy, security and enforcement rules. These changes, for example, make it clear that business associates must comply with HIPAA.
- The Breach Notification Rule. An interim final version is already in effect. OCR withdrew a proposed final version of the rule last year for further consideration. Some observers speculated that the office may be reconsidering the controversial "harm standard" in the interim final version of the rule, which enables organizations to conduct a risk assessment to determine whether a security incident merits a significant risk of harm and thus merits reporting.
- The Enforcement and Compliance Interim Final Rule. As above, an interim final version is already in effect. This will formalize higher penalties for HIPAA violations.
- The GINA proposed rule, Genetic Information Nondiscrimination Act of 2008, (protects patients' genetic information). Privacy provisions under the Genetic Information Nondiscrimination Act. These provisions will formalize that using genetic information for insurance underwriting purposes is a privacy violation as well as a non-discrimination violation, McAndrew said.

McAndrew stated: "We want to ensure that when we do the final HITECH action it contains as much activity as we can." The omnibus final rule will cover new information protection requirements for:

- business associates and subcontractors
- electronic access
- research authorizations
- student immunization records
- restrictions on marketing
- restrictions on fundraising
- prohibition on sale of protected health information

McAndrew added that a separate proposed rule will be issued after the omnibus regulation, and will govern accounting for disclosures (AOD) even for payment, treatment and health plan operations. McAndrew is quoted as saying that the AOD proposed rule is "very close" to being ready. Once that notice is issued, OCR will accept comments before issuing a proposed rule.

The HITECH Act called for a rule outlining how to provide patients with an accounting of the disclosure of electronic records to those outside the organization that created the records. But McAndrew acknowledged that writing the rule is challenging, because of the gray areas involved. "In some hospitals, where many of the practicing physicians really are not part of the hospital entity itself, technically what would seem to be a 'use' of the hospital's electronic health record is actually a 'disclosure' to the physician. So that's one of the issues that's being dealt with."

Meanwhile, OCR is working closely with the HHS Office of the National Coordinator for Health Information Technology to determine whether additional rules, or guidance about compliance with existing rules, are needed to ensure health information remains secure, McAndrew said. In some cases, regulators will need to "find new ways to protect against new vulnerabilities," she added.

Anthony J. Munns, CISA, FBCS, CITP - Partner, Risk Services
Brown Smith Wallace LLC, Phone: 314-983-1297

