

## HAVE YOU HEARD? HIPAA'S BACK WITH A VENGEANCE

ARRA HIPAA. No, we didn't say, "Aarghhhhhhhhhhhh! HIPAA!" (although we've felt it). It's ARRA HIPAA. As in "The American Recovery and Reinvestment Act," Pub. L. 11-5, which you've already heard a great deal about in changing your withholding tables and tweaking and re-tweaking your COBRA administration. Now that the ultra-time-sensitive COBRA periods have passed, it's time to turn your attention back to HIPAA, a subject that caused great upheaval in the beginning years of this decade and is now back with a vengeance.

### Background

Let's start with a refresher course: The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") amended portions of five federal statutes related to group health plan administration: the Employee Retirement Income Security Act ("ERISA"), the Internal Revenue Code, the Public Health Services Act, the Social Security Act ("SSA"), and Title 18 of the U.S. Code. A narrow but significant portion of the vast enactment was entitled, ironically, the "Administrative Simplification" provisions, and these included requirements for maintaining the privacy and security of medical information.

Interestingly, the actual statute passed by Congress had virtually no details in it about how privacy and security were to be protected and maintained; Congress left it to the U.S. Department of Health and Human Services ("HHS") to flesh out the requirements through regulations. HHS therefore issued final Privacy Regulations – which were very detailed – in December 2000. Most health plans had to comply with the regulations by April 2003, with small health plans (defined in 45 C.F.R. § 160.103 as "a health plan with annual receipts of \$5 million or less") having another year. Final HIPAA Security Regulations – which were not as specific as the Privacy Regulations, but perhaps carried more weighty responsibilities – went into effect in April 2003, and the compliance deadline for most group health plans was April 21, 2005, with small group health plans having until April 21, 2006 to achieve compliance.

In essence, the **Privacy Regulations** addressed under which circumstances and in what manner entities and organizations covered by HIPAA could use and disclose Health Information and Protected Health Information, as defined in the regulations. They further prohibited the use or disclosure of such information, other than in a manner expressly allowed or required by the regulations. Additionally, the **Security Regulations** sought to ensure the integrity, security, and availability of electronic protected health information ("EPHI") that is identifiable to an individual by regulating how plans and other covered entities handle EPHI when it is being stored and transmitted.

### The American Recovery and Reinvestment Act

ARRA substantially amends HIPAA's administrative simplification rules. The new Privacy and Security Regulations will require group health plans and other HIPAA-covered entities to make significant modifications to their policies, procedures, and business associate relationships. They will also require business associates to tackle compliance issue with a greater sense of urgency than before.

The health information technologies (“IT”) portions of ARRA are known as the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act creates several new agencies and committees that will have some effect on group health plans in the future. ARRA HIPAA also includes approximately \$24 billion dollars in expenditures in the next decade to fund both incentives for using electronic health records (you’ll see these referred to as “EHRs”) and the development of standards for these and other electronic advances.

ARRA tightens some existing HIPAA provisions, such as marketing and individual rights, and creates some entirely new obligations. As was the case with the initial round of HIPAA-hoopla, employers who sponsor fully-insured plans will see few changes related to the new rules, while self-insured plan sponsors will need to revisit their privacy notice, policies and procedures and will most likely need to update their compliance program.

The biggest change, perhaps, will come to business associates who in the past were only on the hook via contract (and perhaps didn’t really dig into the nuances of HIPAA-compliance as did covered entities). The HITECH Act extends liability under certain HIPAA rules **directly** to the business associates of covered entities. This means that third-party administrators and other business associates are covered directly by HIPAA and the requirements and civil and criminal penalties will apply to business associates beginning in February 2010. As a result, employer-sponsored group health plans will have to review their relationships with business associates, such as third-party administrators, and may need to amend many of their business associate agreements. It may also mean employer-sponsored group health plans find that some vendors and business partners are more resistant to receiving information which could be PHI; they will (or should) be more cautious about inadvertently becoming covered by the Privacy and Security Regulations.

In what is touted as perhaps the most important modification of the Act to covered entities when it comes to protecting private information, new breach notification requirements will require that individuals be notified of any security breaches and, under certain circumstances, that HHS and the media be notified as well. This portion of ARRA HIPAA creates a new definition of “unsecured protected health information.” HHS has issued proposed rules regarding what constitutes “unsecured protected health information” and, essentially, any PHI that is not encrypted or destroyed is “unsecured.”

Covered entities and business associates must comply with most of the new requirements by February 17, 2010, and the breach notification provisions will likely take effect sooner.

With regard to enforcement, ARRA did not go so far as to give individuals a private right to sue, but the HIPAA amendments in ARRA do authorize state attorneys general to enforce HIPAA. The civil monetary penalties – which were hefty to begin with – have also been bolstered, with penalties that can go all the way to a minimum of \$50,000 per violation and up to \$1,500,000 a year (for violations that were due to “willful neglect” and not corrected). These new penalties have **taken effect immediately**.

Importantly, in the category of important NON-changes, the HITECH Act does not change the analysis involved in deciding whether individual health information is the group health plan’s information or employment information (which should be treated as confidential,

but does not fall under HIPAA). This means that return-to-work slips and pre-employment drug screens are still not HIPAA issues, and also means that ARRA HIPAA didn't help us any on some of the muddy issues (like whether enrollment information is protected or not – err on the side of protection).

**HOLD THE DATE:** We have scheduled a Webinar for June 25, 2009 from 9:30-11:30 to discuss ARRA HIPAA. We will go into detail on the changes, discuss the action plan for employers, and will discuss which deadlines apply to which changes. We will also spend some time reviewing the requirements of HIPAA's Privacy and Security Regulations. Stay tuned for more details.