Poyner Spruill LLP
ATTORNEYS AT LAW

HIPAA and HITECH Act

The Stakes Have Gotten Higher for Group Health Plans

06.07.2010

Elizabeth H. Johnson
Nancy C. Brower

Health plan sponsors have long been aware of the HIPAA privacy and security rules that apply to their employee's protected health information (PHI). More recently, the HITECH Act added several new obligations, including breach notification requirements. These changes have made HIPAA compliance a much higher-stakes proposition. The HITECH Act empowers state attorneys general to enforce HIPAA violations, directs HHS to conduct HIPAA compliance audits, and increases penalties for HIPAA noncompliance from an annual per-provision maximum of $25,000 to $1.5 million. HHS and state attorneys general are taking their new enforcement role seriously, the former having announced it will conduct an audit of every entity reporting a breach that affects more than 500 people, and the latter having already pursued at least one enforcement action. With the compliance stakes raised so substantially, let's consider some of the more pressing requirements and what you can do about them.

Develop a written breach response procedure. The new breach notification rule requires both a written response procedure and employee training. The procedure should take into account how you will provide required notifications to affected individuals, HHS and, in some cases, the media. Ideally, it will also account for existing state breach notification laws that may also apply.

Ensure Security Rule compliance. Security Rule compliance is particularly important in order to prevent potential breaches. And, if you are compliant but have a breach anyway, making sure your program is "regulatory ready" (i.e., fully documented) will be helpful to show that the incident occurred despite your best efforts. In past breach-related enforcement actions where security was deemed lacking, regulators have charged penalties as high as $2.25 million, required implementation of a comprehensive written information security program, and required biennial third party audits of that program over a period as long as 20 years.

Update your business associate agreements. In addition, the HITECH Act requires business associates to fully comply with the HIPAA Security Rule and imposes several other obligations. As a result, updating all of your business associate agreements is mandatory. It's also a good idea to think about other provisions that increase protections, particularly in a breach situation. Under the law, your business associates need only notify you if they have had a breach; providing notifications to affected individuals and the cost of mitigating and responding will be left with your organization if the contract does not provide otherwise.

Review your HIPAA policies, procedures and training. With the myriad of legal changes, evolving security technologies, and significantly increased enforcement, this is a great time to review your HIPAA compliance program.

(Periodic reviews of your security compliance are mandatory.) Although maintaining an up-to-date program is certainly a concern for self-insured health plans, employers with fully-insured plans should also have HIPAA policies and procedures in place if they assist employees with resolution of medical claims, or offer other covered plans like certain wellness programs.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075