New Changes Made to HIPAA Privacy and Security Rules

Health and Human Services has issued final regulations that address recent legislative changes to the HIPAA privacy and date security rules. Compliance by employers will be required by Sept. 23, according to a press release.

- By Max Mihelich

The U.S. Department of Health and Human Services released final regulations that address the recent legislative changes made to the Health Insurance Portability and Accountability Act's privacy and data security rules.

Also known as HIPAA, the changes incorporate privacy and data security rules from the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, according to an HHS release.

The majority of the new regulations prohibit the sale of protected health information and the use of it for marketing and fund-raising purposes, the release states.

A new standard will also be applied to how to determine what qualifies as a breach of unsecured PHI by a health plan or a business associate. Under the new rules a breach will be presumed to have occurred unless the health plan or business associate demonstrates that there is a low probability that the PHI has been compromised, according to the statement.

Health plans no longer need to place business associates under contract to maintain the confidentiality of the plan's PHI. HIPAA's privacy and data security rules now directly apply to business associates, as do the law's civil and criminal penalties, the release explains.

According to the release, for each potential breach, a new rule requires a formal risk assessment. If a breach is found to have occurred, the offending health plan is required to notify each affected individual within 60 days of the discovery of the breach, according to the statement.

The new rules take effect March 26 with a compliance date of Sept. 23, the release states.

The entire release can be found here.