HHS toughens HIPAA violation penalties

BY AMANDA MCGRORY-DIXON
April 9, 2013

The U.S. Department of Health and Human Services is implementing tougher penalties for violations of the Health Insurance Portability and Accountability Act.

Before the passage of the Health Information Technology for Economic and Clinical Health Act, civil monetary penalties could total $100 per violation and a maximum aggregate penalty of $25,000 per year for each violation. Typically, civil penalties were only applied in egregious cases; however, as part of the HITECH Act, the final rule increases fines for civil penalties and now includes a tiered penalty structure in line with the nature and circumstances of the violation.

As part of the final rule, the maximum penalty for a HIPAA violation comes to $1.5 million while the assessed penalty relates to the level of culpability characterizing the violation. This includes:

- When the covered entity or business associate is unaware of the violation and would not have known of the violation by exercising reasonable due diligence, a civil penalty of $100 to $50,000 per violation could be distributed.
- If reasonable cause leads to a violation, the civil penalty could come to $1,000 to $50,000 for each violation.
- Following a violation of willful neglect that has been corrected within 30 days of discovery, a civil penalty could total $10,000 to $50,000 per violation.
- For a violation of willful neglect that was not correctly addressed within the required time frame, the civil penalty could be $50,000 to $1.5 million per violation.

If multiple HIPAA violations occur, penalties could surpass $1.5 million.

The final rule also gives affirmative defense for all tier-one violations, defined as unknowable violations, as well as tier-two violations, which are of reasonable cause, when corrected within 30 days of the date after the violation becomes known. Depending upon the nature and extent of the covered entity or business associate's failure to comply, some discretion is allowed to span past the 30-day time frame.

Under the final rule, HHS also does not have to try to informally settle complaints. HHS now can determine whether it will attempt to do so or begin the formal penalty assessment process immediately. HHS can share information found during all investigations and compliance reviews with other law enforcement agencies.

For HIPAA violations by self-funded group health plans, the final rule allows civil penalties to be applied against a covered entity by a business associate acting as its agent. When evaluating the existence of an agency relationship, HHS can practice federal common law principles over a covered entity's right or authority to control a business associate when deciding whether the business associate is acting as an agent.