$750,000 HIPAA Settlement Reinforces Need to Be Proactive

posted on: Monday, September 14, 2015

As the Department of Health and Human Services’ ("HHS") Office of Civil Rights ("OCR") proceeds with its second round of HIPAA audits, this time covering business associates as well as covered entities, a recent settlement with a physician group providing cancer care services serves as a reminder that failure to take HIPAA security seriously can result in hefty fines and a supervised corrective action plan.

The issue began on July 19, 2012, when a laptop bag was stolen from an employee’s car. Although the laptop itself did not contain any electronic Protected Health Information ("ePHI"), backup media for a computer server was also in the bag. That backup media contained the ePHI of approximately 55,000 individuals and was unencrypted. As required, the covered entity, a cancer care physician group, reported the breach to OCR. OCR conducted an investigation and, as a result of that investigation, alleged that the covered entity had: (1) "failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities" to the PHI; (2) "failed to implement policies and procedures that govern the receipt and removal of [ePHI] into and out of its facility; and (3) "impermissibly disclosed" ePHI by failing “to safeguard unencrypted back-up tapes. . . ." The outcome, three years after the initial breach, was a $750,000 fine and a corrective action plan.

The corrective action plan is in effect for three years and requires the covered entity to submit certain information to HHS for approval by HHS. Specifically, the corrective action plan requires the covered entity to conduct a comprehensive and thorough risk assessment within 90 days after the "effective date" of the agreement. The covered entity must provide a copy of that risk assessment to HHS for review. HHS will then inform the covered entity whether it approves or disapproves of the risk assessment. If HHS disapproves of the risk assessment, the covered entity has 60 days to revise its risk assessment to address HHS’s concerns, and then it must resubmit the assessment. The submission/review process continues until HHS approves the risk assessment submitted.

Once HHS approves the risk assessment, the covered entity then has 90 days to submit a risk management plan for HHS’s approval. Once again, the review and approval process takes place until HHS approves the covered entity’s risk management plan. After the approval of the risk management plan, the covered entity must provide HHS with copies of appropriately revised policies and procedures (to the extent revision is necessary based on the risk management plan). Once again, the review process continues until HHS approves the revised policies. The covered entity must do the same with its training program.

In addition, under the corrective action plan, the covered entity submits reports annually and must notify HHS of “Reportable Events.” A “Reportable Event” is broadly defined as any instance in which a workforce member fails to comply with the covered entity’s privacy and security policies. Notably,
any breach of the corrective action plan exposes the covered entity to potential additional civil monetary penalties.

The current action emphasizes OCR’s findings and concerns expressed during Phase 1 of its HIPAA audits. Those audits identified various areas of frequent noncompliance with HIPAA standards, including: risk analysis and risk management, individual access and access control, the reasonable safeguards requirement (including encryption and decryption), device and media controls, transmission security, training, and content and timeliness of breach notifications. OCR indicated that these noncompliance areas would form the foundation of the Phase 2 audits. The alleged deficiencies for which the recent fine was imposed fall squarely within the Phase 2 priorities.

The penalty and corrective action plan serve as a reminder to both covered entities and business associates to ensure that risk assessments and policies are up to date, are well documented, and provide for adequate safeguards for the nature and scope of the business involved.

©2015 Epstein Becker & Green, P.C. All rights reserved.

Source URL: http://www.natlawreview.com/article/750000-hipaa-settlement-reinforces-need-to-be-proactive