Wyrick Robbins Yates & Ponton LLP
4101 Lake Boone Trail, Suite 300
Raleigh, NC 27607
919.781.4000
www.wyrick.com

OCR HIPAA Enforcement and the Future of Mega-Dollar CMPs and Settlements

May 24, 2019

OCR just announced its most recent HIPAA settlement, this time with an EMR vendor Medical Informatics Engineering, acting as a business associate. The enforcement action relates to a 2015 data breach caused by compromised user credentials. Consistent with recent trends, the agency continues to focus on the requirement to conduct an accurate and thorough enterprise-wide risk analysis, as set forth in the HIPAA Security Rule. In this case, the resolution agreement directly attributes the non-compliance to the vendor's failure to meet that requirement. OCR Director Severino also added, "[t]he failure to identify potential risks and vulnerabilities to ePHI opens the door to breaches and violates HIPAA." The message is once again reinforced that covered entities and business associates must prioritize their on-going risk analyses to evaluate potential threats to the confidentiality, integrity, and availability of PHI. This settlement also serves as a reminder that business associates are directly subject to OCR enforcement for failure to meet the requirements of the HIPAA Security Rule.

The dollar amount of this settlement also presents some interesting considerations. Earlier this spring, on the heels of a record-breaking year of enforcement activities totaling $28.7M in settlements and penalties, HHS issued a notice that it will lower the maximum civil monetary penalties for certain HIPAA violations. The agency noted that this exercise of enforcement discretion would be effective immediately and indefinitely. At the time of the announcement, OCR Director Severino indicated the agency hopes to create a "culture of compliance" rather than penalize entities. In line with that sentiment, the revised penalty limits are greatly reduced for entities with lower levels of culpability while the limit for more egregious violations (willful neglect) remains unchanged.

Notably, even if we see a reduction in CMPs as a result of the revised caps, OCR settlement agreements are not subject to the same culpability-based framework and limits as the CMPs. Entities agree to pay the settlement amounts and implement agency-imposed corrective action plans in hopes of avoiding

Related Attorneys

Tara N. Cho
tcho@wyrick.com

penalties. OCR commentary and enforcement activities have historically suggested that when determining settlement amounts, the agency considers the size, scope and financial status of the entity (i.e., ability to pay) and also the nature of the violations. For example, this most recent settlement with Medical Informatics Engineering for $100,000 is related to a breach affecting 3.5M patients. OCR's $3M settlement with a diagnostic medical imaging company (covered entity) announced earlier this month stemmed from a breach involving virtually the same data elements (same level of sensitivity) and affected 300,000 patients. Although its breach affected a much smaller number of patients, the covered entity had more allegations of non-compliance that were also more serious in nature. If we assume the covered entity also has a higher annual revenue, these contrasting outcomes are not surprising. However, given that Medical Informatics Engineering is also paying out $900,000 in a separate consent judgment to settle a suit by 16 state attorneys general, it could be that these entities actually have similar revenue but OCR factored in the states' settlement to land at a total of $1M.

The majority of OCR enforcement actions result in resolution agreements as opposed to CMPs, but it may be too soon to tell how the new caps might influence OCR's enforcement discretion. For example, entities with higher revenues may try to leverage the new caps to press for lower settlement amounts when negotiating resolution agreements; however, increased enforcement by states may counteract that tactic. Although OCR has indicated creating a culture of compliance is priority over pure punishment, non-compliant entities may still face high-dollar stakes from combined state and federal enforcement actions.