SQUIRE PATTON BOGGS

Court Vacates OCR HIPAA Penalty, Limits OCR Enforcement Authority

US – February 2020

The Fifth Circuit Court of Appeals recently handed down a landmark decision criticizing and restricting how the Department of Health and Human Services Office of Civil Rights' (OCR) interprets HIPAA and OCR's penalty authority.

OCR brought an enforcement action against the University of Texas M.D. Anderson Cancer Center (M.D. Anderson) stemming from three alleged data breaches and violations of various HIPAA requirements. OCR imposed a US$4,348,000 penalty, which M.D. Anderson appealed up to the Fifth Circuit. In rejecting the penalty, the Court criticized not only OCR's interpretation of the HIPAA regulations generally but also OCR's penalty calculation in this case.

(1) The HIPAA Security Rule Encryption Requirement. The Court first interpreted the HIPAA Security Rule requirement to encrypt ePHI. OCR claimed that MD Anderson violated this requirement because it adopted a policy to encrypt portable media, which was not implemented on the devices at issue. The Court, however, ruled that HIPAA only requires Covered Entities to implement a "mechanism" to encrypt data. Here, the Court found that M.D. Anderson had adopted a "mechanism" to encrypt (through its policy requiring such encryption) even if that "mechanism" was not perfectly implemented. In other words, the failure to fully implement the encryption policy did not itself violate the HIPAA encryption requirement.

(2) The HIPAA Privacy Rule Prohibition on Unauthorized Disclosures. The Court next held that the Privacy Rule prohibition on unauthorized "disclosures" is only violated when there is an affirmative act of disclosure, rather than a general loss of data. According to the Court, the mere "loss of control" of PHI (e.g., when a device is stolen), therefore, does not constitute an unauthorized "disclosure." This position mirrors how California courts have interpreted similar provisions in the analogous state Confidentiality of Medical Information Act ("CMIA"). See, e.g., *Sutter Health v. Superior Court*, 174 Cal. Rptr. 3d 653 (Cal. 3d Dist. Ct. App. July 21, 2014).

The *M.D. Anderson* Court further held that OCR's penalty was arbitrary and capricious because OCR had not imposed penalties on entities in similar cases. Finally, the court also found that OCR incorrectly applied the statutory penalty caps for multiple identical violations in a single year (though OCR had already conceded that issue through a "Notice of Enforcement Discretion Regarding HIPAA Civil Money Penalties" in 2019).

This decision is a dramatic rebuttal of how OCR has historically enforced HIPAA and could have far-ranging consequences. Although the decision may force OCR to interpret violations more narrowly and seek lower penalties, OCR may counteract such limitations by more aggressively identifying potential violations during investigations to extract settlements and avoid litigation altogether. The decision, coupled with a changing administration, means increased enforcement uncertainty, so Covered Entities and Business Associates should take this opportunity to review their HIPAA compliance efforts.

If you have any questions, please contact the authors of this article or your regular contact from the firm.

Contacts

Elliot R. Golding
Partner, Washington DC
T +1 202 457 6407
E elliot.golding@squirepb.com

Kristin L. Bryan
Senior Associate, Cleveland
T+1 216 479 8070
E kristin.bryan@squirepb.com

Christina M. Lamoureux
Associate, Washington DC
T +1 202 457 6095
E christina.lamoureux@squirepb.com

40508/02/21