THOMPSON COBURN LLP

insights

TYPES NOT MAPPED YET February 23, 2021 | TTR not mapped yet | Milada R. Goturi

Fifth Circuit vacates $4.3M HHS enforcement penalty for HIPAA violations

Last month, the US Court of Appeals for the Fifth Circuit issued a ruling vacating a $4.3 million civil monetary penalty (CMP) against the University of Texas MD Anderson Cancer Center (Anderson) by the US Department for Health and Human Services (HHS) for alleged violations of the HIPAA Privacy and Security Rules. The case originated from three separate voluntary breach reports made by Anderson to HHS in 2012 and 2013, involving one stolen unencrypted laptop and two lost unencrypted USB drives, which contained among them the electronic protected health information (ePHI) of over 34,000 individuals.

The Court offered a scathing review of HHS's enforcement action, explaining that HHS's fine against Anderson was "arbitrary, capricious, and otherwise unlawful… for at least four independent reasons."

First, the Court criticized HHS's interpretation of the Security Rule's requirement that all covered entities "implement a mechanism to encrypt and decrypt [ePHI]." The Court found that the rule does only as it plainly states – requires the covered to implement "a mechanism" for encryption – and concluded that Anderson did just that. In doing so, the Court rejected HHS's arguments that Anderson's failure to actually encrypt the three devices involved in the breaches was a violation of this encryption requirement, stating the regulation "does not require a covered entity to warrant its mechanism provides bulletproof protection of all systems containing ePHI."

Second, the Court disagreed with HHS's interpretation of the regulations prohibiting a covered entity from disclosing ePHI except as permitted by the HIPAA Privacy Rule. Where HHS argued that "disclosure" under the HIPAA Rules occurs when there is a "loss of control" of devices containing ePHI, the Court concluded that the ePHI must affirmatively be transferred to an individual outside the covered entity. The Court went on to reject HHS's argument that such a standard would be too difficult for the agency to meet.

Third, the Court noted that HHS "arbitrarily and capriciously" enforced the CMP rules over Anderson while other covered entities face zero financial penalties, explaining that "a bedrock principal of administrative law is to treat like cases alike."

Finally, the Court took issue with and vacated the $4.3 million penalty amount that HHS imposed on Anderson as exceeding the penalty caps set by Congress in the HIPAA statutes. The Court observed that the HIPAA violations at issue were found to be attributable to "reasonable cause" and not "willful neglect" and that the statutory cap for such violations was $100,000 for all violations of the identical requirement. The Court also observed that in this case HHS itself conceded that it only had authority to issue a fine up to $450,000 based on the statutory penalty limits.

While covered entities should take note of the guidance offered by the ruling, the extent of the impact of the ruling, particularly on how HHS will enforce similar incidents in the future, remains to be seen.

authorsTest

milada

Milada R. Goturi