Data Privacy and Cybersecurity

Fifth Circuit Vacates $4.3M in HIPAA Civil Penalties Offering New View of HHS Regulations

By: David P. Saunders and Allison N. Glover

On January 14, 2021, the Fifth Circuit vacated a $4.3 million penalty imposed by the US Department of Health and Human Services (HHS) on M.D. Anderson Cancer Center (M.D. Anderson) in connection with three data incidents experienced by the center. *University of Texas M.D. Anderson Cancer Center v. United States Department of Health and Human Services*, No. 19-6022 (5th Cir. January 14, 2021). In vacating the penalty, the Fifth Circuit held that (1) HHS had not shown that the loss of unencrypted electronic protected health information (PHI) on its own was sufficient to demonstrate a breach of any HIPAA rules and (2) the penalty imposed on M.D. Anderson was arbitrary, capacious, and unlawful because it exceeded HHS' authority. *Id.* The Court's decision potentially will have ripple effects for the future of HIPAA enforcement actions, including potentially spurring HHS to create new regulations. In the meantime, the *University of Texas* ruling could mean that fewer companies will report lost or stolen devices as a HIPAA data breach, turning on its head years of prior practice. Either way, the Fifth Circuit's decision is a big one in terms of HIPAA enforcement.

In 2012 and 2013, M.D. Anderson reported the theft of an unencrypted laptop and the loss of two unencrypted USB drives that contained the PHI of over 34,000 individuals to HHS. Following an investigation of the reported breaches, HHS concluded that M.D. Anderson had violated the encryption and disclosure rules under HIPAA because the devices were not encrypted, and contained PHI. 45 C.F.R. §§ 164.312(a)(2)(iv), 164.306(d), 164.502(a). The Fifth Circuit disagreed, however, finding dispositive the fact that M.D. Anderson *had* an encryption policy, period: "nothing in HHS' regulation says that a covered entity's failure to encrypt three devices means that it has never implemented 'a mechanism' to encrypt anything at all," as required by the HIPAA rules. *University of Texas M.D. Anderson Cancer Center*, No. 19-6022 at 7. Thus, because M.D. Anderson had a mechanism for encryption, it had not technically violated the HIPAA rules according to the Fifth Circuit. And even if the failure to encrypt *had* violated the HIPAA rules, the *University of Texas* court took things a step further and held that in order to prove a breach of PHI, HHS must demonstrate "an affirmative act of disclosure, not a passive loss of information." *Id.* at 9. In other words, the mere theft of an unencrypted device with PHI on it was not enough for HHS to carry its burden; it was required to somehow show that the thief actually accessed the PHI on the stolen devices. Ultimately, because HHS could not prove that the thief or someone else actually obtained the PHI on the three stolen devices, HHS could not impose a penalty on M.D. Anderson. *Id.* at 9-10. The burden of proof imposed by the Fifth Circuit makes it difficult to imagine *any* scenario of theft of information in which HHS could prove that a breach led to an unauthorized disclosure of PHI and, in the process, stands on its head more than a decade of understanding and practice related to HIPAA enforcement.

Even if HHS had been able to meet its burden of proof, the Fifth Circuit held that the $4.3 million penalty imposed on M.D. Anderson was arbitrary and capricious because HHS only had the authority to issue a fine of up to $450,000 for a reasonable cause violation. *Id.* at 14. The Fifth Circuit therefore vacated the $4.3 million penalty. *Id.* at 15.

The Fifth Circuit's *University of Texas* opinion has both practical short and long term impacts on HIPAA enforcement. In the near term, the opinion identifies a very high standard by which HHS must prove that stolen or lost PHI was actually disclosed in an unauthorized fashion. And for businesses, the ruling could have a practical impact. If the Fifth Circuit's opinion holds, then just because an unencrypted

device containing PHI is lost or stolen, it may not mean that a business has to report that loss or theft as a HIPAA data breach. In the last 24 months alone, there have been 25 reports through the HHS Office for Civil Rights reporting data breaches of precisely this variety. *See* US Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to Secretary of HHS Breach of Unsecured PHI. The *University of Texas* opinion calls into question whether the business needed to file these reports. In the longer term, the Fifth Circuit's opinion likely means that businesses should expect more rule making from HHS to close the perceived gap through which the Fifth Circuit reached its conclusion. In the meantime, however, businesses now have a new arrow in their quiver when it comes to defending their practices and concluding that the loss of PHI may not have been a violation of any provision of HIPAA.

Contact Us

David P. Saunders

dsaunders@jenner.com | Download V-Card

Allison N. Glover

aglover@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower

Chair

dbitkower@jenner.com

Download V-Card

David P. Saunders

Co-chair

dsaunders@jenner.com

Download V-Card