

Recent Case Impacts HIPAA and HITECH Act Penalties

By: Debra A. Weinrich and L. Stephen Bowers

Healthcare Industry Alert

2.1.21

The U.S. Department of Health and Human Services (HHS) enforces the privacy and security provisions of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (the HITECH Act). HHS has a history of imposing staggering penalties under HIPAA and/or the HITECH Act, usually where failures were egregious or where the covered entity failed to correct issues raised by HHS. However, a recent case in the Fifth Circuit Court of Appeals curtailed HHS's authority to punish self-reported HIPAA violations arising from the theft or inadvertent loss of Protected Health Information (PHI) where there is no proof of any improper recipient of the private information.

The case of *University of Texas M.D. Anderson Cancer Center vs. U.S. Department of Health and Human Services* relates to the Anderson Cancer Center's attempts to appeal the assessment of a \$4.3 million penalty assessed for several inadvertent violations of HIPAA. Specifically, devices containing PHI were lost or stolen on three separate, unrelated occasions. Although Anderson had a specific policy in place requiring encryption of such devices, it appears the policy was not universally enforced or followed, and the devices at issue were not appropriately encrypted.

HHS took the position that the failure to ensure that PHI maintained in an electronic form (e-PHI) was protected by encryption demonstrated that Anderson did not have such a mechanism, and imposed a massive penalty. Anderson unsuccessfully appealed the assessment of the penalty through several levels of administrative review, and finally petitioned the court for judicial review of HHS's decision to assess the penalty.

The Fifth Circuit's opinion is scathing. It notes that HHS, early in the proceedings, admitted that the penalty was indefensible, and offered to reduce it to approximately 10% of the amount originally assessed. However, the court went even farther and determined the entire penalty was arbitrary and capricious, and that it went beyond HHS's authority to assess, based upon the plain language of HHS's own regulations.

- First, the court goes to great lengths to emphasize that HHS regulations requiring an encryption mechanism mandate a "mechanism," but do not require that such a mechanism be "bulletproof." Where, as here, a mechanism is established and reasonable, but not 100% effective, the court indicates HHS is unable to show a violation of the plain language of the regulation.
- Second, the court rules that an inadvertent loss of a device containing e-PHI cannot be considered a "disclosure" of e-PHI in violation of HHS regulations. Although HHS's position is that any "loss of control" of e-PHI constitutes a "disclosure," the court found that interpretation is unsupported by the language of the regulation.
- Third, the court criticized HHS and the administrative tribunal that upheld the penalty for failing to compare HHS enforcement in the *Anderson* case to similar cases. *Anderson* presented evidence of a number of similar cases which did not result in an assessment of penalties, let alone penalties of a similar magnitude. The court indicated HHS's failure to demonstrate specific, articulated differences between the cases which would warrant the difference in enforcement penalties rendered its decision arbitrary and capricious.
- Finally, the court addressed the amount of the penalties. Although HHS essentially conceded it had overreached in assessing the larger penalty, the court specifically outlines the statutory and regulatory guidance which limits the amount of the penalty that can be assessed. Although HHS offered to reduce the penalty based on "enforcement discretion," the court decision indicates HHS's

discretion is strictly limited by the language of the laws.

The *Anderson* decision greatly erodes several long-held HHS contentions. Although the enforcement provisions of HIPAA and the HITECH Act are intimidating, the decision demonstrates they are not without limit. A covered entity threatened by enforcement action should be prepared to evaluate its ability to challenge HHS's discretion. This case provides a roadmap for such challenges.

Our privacy and healthcare lawyers counsel clients on HIPAA and the HITECH Act and, when necessary, litigate them in both administrative and judicial forums. If you have questions or would like more information, please contact Debra Weinrich (weinrichd@whiteandwilliams.com; 215.864.6260).

This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only and you are urged to consult a lawyer concerning your own situation and legal questions.