Fifth Circuit Vacates HIPAA Penalty Against M.D. Anderson

Related Attorneys

J. Liam Gruzs

Related Industries

Health Care

CLIENT ALERT | 1.20.2021

In a January 14, 2021 ruling, the U.S. Court of Appeals for the Fifth Circuit ("Fifth Circuit") vacated a $4.3 million Health Insurance Portability and Accountability Act of 1996 ("HIPAA") fine against the University of Texas M.D. Anderson Cancer Center ("M.D. Anderson"), finding the penalty "arbitrary, capricious and contrary to law." This decision vacates the ALJ decision affirming HHS's imposition of the civil monetary penalty ("CMP") against M.D. Anderson following a loss and theft of unencrypted devices containing patient data.

In June 2018, the U.S. Department of Health and Human Services ("HHS") imposed a CMP in the amount of $4.3 million against M.D. Anderson after completing an investigation of three data breaches involving the theft of an unencrypted laptop and the loss of two unencrypted flash drives between 2012 and 2013. The laptop and flash drives collectively contained the electronic protected health information ("ePHI") of approximately 35,000 patients. HHS found that M.D. Anderson failed to implement encryption or adopt an alternative and equivalent method to limit access to ePHI stored on electronic devices, and allowed for the unauthorized disclosure of ePHI. HHS also determined that M.D. Anderson had "reasonable cause" to know that it had violated HIPAA.

M.D. Anderson unsuccessfully contested the penalty through two levels of administrative appeals before petitioning the Fifth Circuit in April 2019. M.D. Anderson argued both that the penalty was excessive, and HHS, a federal agency, did not have the authority to impose civil monetary penalties against M.D. Anderson, a state agency.

The Fifth Circuit held that the CMP violated the Administrative Procedure Act because HHS's actions were "arbitrary, capricious, and otherwise unlawful" for four reasons:

1. M.D. Anderson had in fact implemented various mechanisms to encrypt ePHI, including an "IronKey" to encrypt and decrypt mobile devices along with employee training on how to use it, a mechanism to encrypt emails and various other mechanisms for file-level encryption. While HHS argued that M.D. Anderson should

have done more, the Court found that the HIPAA Security Rule merely requires "a mechanism" and does not require "bulletproof protection of all systems containing ePHI";

2. The text of the HIPAA Privacy Rule defines a disclosure as "the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information," and M.D. Anderson did not affirmatively act to disclose PHI and HHS did not prove that someone outside the entity received the information;
3. The CMP violated the bedrock principal of administrative law that an agency, such as HHS, must "treat like cases alike." Unlike the multi-million dollar penalty imposed upon M.D. Anderson by HHS, the Fifth Circuit found that several other covered entities had similar breaches and faced zero financial penalties, for which HHS "offered no reasoned justification"; and
4. The penalty amounts contradicted the HIPAA Enforcement Rule, which limits all penalties within a calendar year for all violations that were attributable to a covered entity's reasonable cause to $100,000.

After M.D. Anderson filed its petition with the Fifth Circuit, HHS conceded it could not defend a fine for the breaches of more than $450,000. The Fifth Circuit vacated the civil monetary penalties and remanded the case for further proceedings consistent with the opinion.

Takeaways:

- While breaches are bound to occur, covered entities and business associates should ensure they are taking proactive measures to protect patient information. This decision shows that courts are likely to be sympathetic to entities that can demonstrate they have implemented safeguards, even if such safeguards were not entirely effective in preventing an unauthorized disclosure.
- The HIPAA Disclosure Rule prohibits a covered entity or business associate from disclosing PHI in a manner not permitted under HIPAA, while the HIPAA Breach Notification Rule requires that covered entities and their business associates provide notification following a breach of unsecured PHI. "Breach" is defined as an impermissible acquisition, access, use or disclosure of PHI not permitted under HIPAA and that compromises the security or privacy of PHI. Based on the Fifth Circuit's finding that there was not an impermissible disclosure by M.D. Anderson, covered entities and business associates may now have an argument that breach notification is not required in situations where unencrypted devices are lost, but it cannot be demonstrated that someone outside of the entity was able to access the PHI on the device.
- This decision may discourage covered entities and business associate from entering into large dollar settlements with HHS, and will certainly encourage other covered entities or business associates to contest any attempt by HHS to impose large CMPs since the Fifth Circuit ruling certainly raises the bar for what HHS must demonstrate to justify a civil monetary penalty.
- It remains to be seen whether HHS will appeal this decision or if HHS will alter how it enforces HIPAA or if it will propose changes to the HIPAA Privacy and Security Rules in light of the Fifth Circuit's ruling.

If you have questions, please contact Lisa Pierce Reisz, Liam Gruzs, Jonathan Ishee, Nita Garg, or your regular Vorys attorney.