Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5th Circ. Creates Roadblocks For New HHS Privacy Enforcers

By **Allison Grande**

Law360 (February 5, 2021, 6:02 PM EST) -- The Biden administration could face a tougher time punishing data security missteps and securing record-setting fines following an unprecedented Fifth Circuit ruling in January that cut down a $4.3 million penalty against MD Anderson Cancer Center.

In a first-of-its-kind challenge to a penalty issued under the Health Insurance Portability and Accountability Act, a unanimous appellate panel slammed the U.S. Department of Health and Human Services for holding MD Anderson to an unreasonably strict encryption standard and imposing a harsh punishment that didn't align with prior enforcement actions or its guidelines for calculating penalties.

"The Fifth Circuit's decision essentially eviscerates HHS' ability to enforce aspects of its HIPAA data security rules and, if it's followed by other courts, signifies that a very demanding level of scrutiny will be applied to future HHS enforcement decisions," said Behnam Dayanim, the head of Paul Hastings LLP's privacy and cybersecurity practice.

HHS' Office of Civil Rights ramped up both the frequency and size of its HIPAA penalties during the past five years, headlined by a record $16 million deal reached in 2018 with health insurer Anthem Inc. over its massive data breach.

The Fifth Circuit's ruling comes as the agency moves to a Democratic administration that's widely expected to take an even more aggressive approach than its predecessor to ensuring health care entities and their business associates are adequately safeguarding patients' sensitive data.

"But now, OCR has to struggle with the challenge of a court telling them that their current process for enforcing HIPAA violations doesn't work," said Adam Greene, a partner at Davis Wright Tremaine LLP and a former privacy adviser at the OCR.

The decision is likely to make the OCR rethink the way it assesses privacy and data security penalties and could motivate the agency to issue regulations clarifying aspects of its enforcement approach that were criticized by the Fifth Circuit, according to attorneys.

"What the Fifth Circuit has essentially said here is that it doesn't like regulation by enforcement action, so if the agency is going to regulate something, it has to say it outright and can't go beyond what the regulation itself says," said Brenda Sharton, global co-chair of Dechert LLP's privacy and cybersecurity practice.

Morgan Lewis & Bockius LLP partner Scott McBride, who represented MD Anderson in the Fifth Circuit appeal, stressed that the case of first impression was at its core about "the lack of consistent and transparent standards in enforcement activities and adherence to actual regulatory enforcement standards by the agency."

"The case is not about avoiding patient privacy and security requirements, which is something supported and promoted by the healthcare industry," he told Law360, adding that the panel's opinion is poised to "impact OCR enforcement actions going forward across the healthcare industry."

In declaring the $4.3 million penalty against MD Anderson to be arbitrary and capricious, the Fifth Circuit found the agency had too broadly read HIPAA's encryption and disclosure rules and had failed to follow the "bedrock principle of administrative law" to "treat like cases alike."

MD Anderson fell into the OCR's crosshairs after disclosing the theft of an unencrypted laptop and losses of two unencrypted USB drives that together contained the electronic personal health information, or ePHI, of more than 33,000 people. The cancer center pointed in its appeal to past instances where entities had been accused of violating the government's understanding of the encryption rule and faced "zero financial penalties."

In one such example, HHS elected to impose "no penalty at all" after Cedars-Sinai reported an employee had lost an unencrypted laptop containing ePHI for more than 33,000 patients in a burglary, according to the panel's opinion.

The OCR countered that it evaluates each case on its individual facts, an approach that's consistent with the "big picture view of compliance" that the agency has long taken. Under this strategy, the agency evaluates not only the choices a company has made, but also how it has adjusted its business practices over time, the lessons it's learned from the incident and its overall history, noted Kirk Nahra, co-chair of the privacy and cybersecurity group at WilmerHale.

The appellate panel's rejection of this broader approach — which the three judges found led to different treatment of similarly situated companies — "is going to lead to OCR being in a tougher posture on enforcement, which may perversely lead to more aggressive and automatic actions with perhaps less thoughtful consideration," according to Nahra.

As a "rough analogy," Nahra pointed to how the Federal Trade Commission has moved to make its data security orders "more specific and often tougher in some situations" in the wake of a 2018 Eleventh Circuit ruling that threw out an order against LabMD due to a lack of specifics about how proposed data security changes should be implemented.

The HHS civil rights agency may similarly be driven to make changes to its enforcement strategy to ensure punishments are being doled out consistently across the board, attorneys say.

"This ruling calls into question whether OCR can continue to make an example out of a small number of companies as it's historically done," Greene said.

According to enforcement statistics on the OCR's website, the agency has settled or imposed a civil monetary penalty in 93 cases it's investigated, while in 28,533 instances it elected to forgo a fine in favor of requiring companies to implement corrective actions or giving them technical assistance.

But while the Fifth Circuit's check on the OCR's enforcement posture may spur the civil rights agency to consider imposing sanctions more frequently, the ruling could also hamper its ability to attach hefty price tags to these actions, attorneys say.

In issuing the contested fine, the OCR found the cancer center to be liable for $2,000 per day from March 24, 2011, to Jan. 25, 2013, for a failure to implement technical procedures and safeguards concerning ePHI and $1.5 million per year for improper use or disclosure of protected health information in 2012 and 2013.

However, the agency conceded in its briefing before the Fifth Circuit that it only had the authority to issue a fine of up to $450,000. This discrepancy resulted from confusion around the yearly cap for such violations. The OCR originally calculated the cap as $1.5 million, but after the Trump administration **moved in April 2019** to sharply reduce maximum annual penalties for less-culpable HIPAA violators, it concluded it shouldn't have exceeded $100,000.

"The discussion of penalties seems reasonably consistent with the statute, but OCR has been trying to build to higher penalties," Nahra said. "This will certainly make that much harder."

Following the Fifth Circuit's ruling, the OCR is likely to be careful about not only double-checking its penalty calculations, but also ensuring the totals they reach can't be dismissed as arbitrary and capricious.

"Part of the challenge for OCR will be figuring out how it can levy penalties in a way that's proportionate to the violation and still promotes OCR's goal to make sure that people in the industry are taking these requirements seriously," said Linda Malek, chair of the health care and privacy and cybersecurity practices at Moses & Singer LLP.

The panel's parsing of the HIPAA encryption and disclosure rules could also make it significantly more difficult for the OCR to recover any penalties against health care companies that find themselves in situations similar to MD Anderson's, attorneys say.

"[The opinion] does support the idea that entities that invest in HIPAA compliance programs should not be penalized just because something goes wrong and, as a result, they properly report a data breach," said Shannon B. Hartsfield, a health lawyer and the executive partner of Holland & Knight LLP's Tallahassee office.

In vacating the contested penalty and sending the matter back to the agency for further proceedings, the Fifth Circuit found the OCR was wrong to determine MD Anderson had failed to meet its obligation to "implement a mechanism to encrypt and decrypt electronic protected health information" or document why it decided not to put in place the specified standard or an equivalent alternative.

The panel found it was "undisputed" that MD Anderson had implemented a "mechanism," pointing to how the cancer center required that portable computing devices be encrypted and how it furnished employees with a key to encrypt such data and trained them on how to use it.

Even though the stolen laptop and lost USB drives weren't encrypted, "that does not mean MD Anderson failed to implement a 'mechanism' to encrypt ePHI" as required by the letter of the regulations, according to the panel.

The OCR has so far taken a rigorous view of this standard, stating informally that it expects covered entities to have encryption at motion and at rest, noted Malek, the Moses & Singer partner.

"This ruling pushes that back a little bit and, if upheld, will pose challenges to enforcement, particularly when it comes to determining what it means to be diligent about making sure covered entities' practices are actually implemented and how far they need to go," Malek added.

Typically, health care providers and their covered vendors don't have a problem with putting an encryption mechanism in place. Rather, they run into trouble with ensuring that the standard is being implemented and enforced as intended across their organizations, according to attorneys.

"What the court seems to be saying here is that, as long as there's a mechanism in place, absent some unusual circumstances, OCR is not able to penalize an entity for a violation," said Dayanim, the Paul Hastings partner.

"That's a much different standard than entities were assuming they were operating under and, if that holding is to be taken at face value, would set a very low bar for regulated entities moving forward," he said.

McBride, the Morgan Lewis partner representing MD Anderson, noted that while healthcare providers "may take some comfort" in the court's "logical conclusion that the regulations do not create strict liability or require a 'bullet proof' mechanism of protection, they should continue to be vigilant in maintaining patient privacy and security."

"We don't expect the decision would lessen any of the focus and vigilance of healthcare providers to continue to protect patient information," he added.

The Fifth Circuit's assessment of the HIPAA disclosure rule is also likely to have a notable impact on how violations are enforced and if the agency is even notified about incidents at all, attorneys say.

Under the rule, health care providers and their business associates are prohibited from releasing, transferring, providing access to or otherwise divulging information to "outside" sources.

In a 2018 ruling upholding the penalty, an administrative law judge at the OCR concluded that covered entities violate the disclosure rule whenever they lose control of protected health information.

But the Fifth Circuit found that interpretation to be a significant departure from the regulation HHS wrote, which uses verbs that suggest "an affirmative act of disclosure, not a passive loss of information," needs to have taken place and requires information to have been disclosed to "someone" who's "outside" the covered entity.

This conclusion "suggests that there is a fairly high bar that the government would need to meet to prove that data went outside the entity, and someone stealing data does not mean that the entity affirmatively acted to disclose the PHI," said Hartsfield, the Holland & Knight partner.

Given these interpretations, it wouldn't be surprising if the MD Anderson decision led to "significantly lower penalties" in situations where workers don't follow their data security training but "there is no proof that health information was accessed by a third party, such as a situation where an employee is

trained to shred hard-copy health information before disposing of it, but fails to do so," noted Angie Matney, senior counsel at Loeb & Loeb LLP.

Moving forward, health care entities are expected to use the Fifth Circuit ruling as a springboard to more aggressively push back on OCR enforcement decisions, according to attorneys.

Of the dozens of HIPAA fines the OCR has imposed since the privacy rule took effect in 2003, MD Anderson is the first to appeal its fine to a circuit court. Attorneys predict the ruling will not only feature prominently in future negotiations with the regulator, but will also embolden companies to mount their own appeals to enforcement outcomes they view as unreasonable.

"The MD Anderson ruling doesn't have impact outside the Fifth Circuit, but what it does do is indicate that health care entities may have some traction if they challenge these fines in other jurisdictions," Malek said.

The OCR could look to stave off such challenges by moving to issue new regulations that address the issues and ambiguities highlighted in the MD Anderson decision, according to Foley Hoag LLP privacy and data security practice co-chair Colin Zick.

"The ruling is likely to be a motivator, because they're being called out," Zick said. "If OCR is thinking strategically and trying to avoid getting beat over the head with this decision in every single case, they've got to think about doing something to change the playing field."

Such action could help the agency move past the MD Anderson decision as it transitions to new leadership.

The agency under the Biden administration is expected to keep the privacy and data security pressure on covered entities, particularly if California Attorney General Xavier Becerra is confirmed to lead HHS.

Like his predecessor and current Vice President Kamala Harris, Becerra has actively pursued alleged privacy and data security violations during his tenure as California's top prosecutor. His office has also been in charge of drafting regulations for and enforcing the state's landmark consumer privacy law, which went live last year and gives consumers more access to and control over their personal information.

"Becerra has a record of aggressively enforcing consumer privacy regulations, so it is reasonable to think he will bring a similar approach to HHS," Matney, the Loeb & Loeb attorney, said.

Additionally, OCR Director Roger Severino left his position on Jan. 15 after nearly four years on the job. Robinsue Frohboese, who's been at the agency since 2000, is currently serving as acting director, a role she's assumed during four administration transitions, according to her bio on the agency's website.

The extent to which the new administration is hampered by the Fifth Circuit's ruling is likely to depend heavily on where it decides to focus its somewhat limited enforcement resources, a target that's likely to look different than it did at the time of the MD Anderson breaches in 2012 and 2013, when the cyberthreat landscape was far from being as sprawling or sophisticated as it is today, according to attorneys.

"The hope is that OCR will give priority in enforcement situations to where there's a real egregious

disregard of the law as opposed to focusing on companies that suffer hacking incidents and are doing their best to comply," said Fox Rothschild partner and HIPAA privacy officer Elizabeth Litten.

Fifth Circuit Judges Jacques L. Wiener Jr., Kurt D. Engelhardt and Andrew S. Oldham decided the appeal.

MD Anderson is represented by B. Scott McBride, John W. Petrelli and David B. Salmons of Morgan Lewis & Bockius LLP.

The OCR is represented in-house by Daniel R. Wolfe, Roger C. Geer, John F. Benevelli and Amita A. Sanghvi.

The case is The University of Texas MD Anderson Cancer Center v. U.S. Department of Health and Human Services, case number 19-60226, in the U.S. Court of Appeals for the Fifth Circuit.

--Editing by Philip Shea and Marygrace Murphy.