United States Court of Appeals for the Fifth Circuit

United States Court of Appeals
Fifth Circuit
FILED
January 14, 2021
Lyle W. Cayce
Clerk

No. 19-60226

UNIVERSITY OF TEXAS M.D. ANDERSON CANCER CENTER,

Petitioner,

versus

UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES,

Respondent.

On Petition for Review of a Final Agency Decision
of the U.S. Department of Health and Human Services

Before WIENER, ENGELHARDT, and OLDHAM, *Circuit Judges*.

ANDREW S. OLDHAM, *Circuit Judge*:

Employees of the University of Texas M.D. Anderson Cancer Center ("M.D. Anderson" or "Petitioner") lost patients' data. In response, the United States Department of Health and Human Services ("HHS" or the "Government") fined M.D. Anderson $4,348,000. After M.D. Anderson filed its petition for review, HHS conceded that it could not defend a fine in excess of $450,000. The Government's decision was arbitrary, capricious, and contrary to law. We grant the petition for review and vacate the penalty.

I.

Three unfortunate events set the stage for this lawsuit. First, back in 2012, an M.D. Anderson faculty member's laptop was stolen. The laptop was not encrypted or password-protected but contained "electronic protected health information (ePHI) for 29,021 individuals." Second, also in 2012, an M.D. Anderson trainee lost an unencrypted USB thumb drive during her evening commute. That thumb drive contained ePHI for over 2,000 individuals. Finally, in 2013, a visiting researcher at M.D. Anderson misplaced another unencrypted USB thumb drive, this time containing ePHI for nearly 3,600 individuals.

M.D. Anderson disclosed these incidents to HHS. Then HHS determined that M.D. Anderson had violated two federal regulations. HHS promulgated both of those regulations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act"). The first regulation requires entities covered by HIPAA and the HITECH Act to "[i]mplement a mechanism to encrypt" ePHI or adopt some other "reasonable and appropriate" method to limit access to patient data. 45 C.F.R. §§ 164.312(a)(2)(iv), 164.306(d) (the "Encryption Rule"). The second regulation prohibits the unpermitted disclosure of protected health information. *Id.* § 164.502(a) (the "Disclosure Rule").

HHS also determined that M.D. Anderson had "reasonable cause" to know that it had violated the rules. 42 U.S.C. § 1320d-5(a)(1)(B) (setting out the "reasonable cause" culpability standard). So, in a purported exercise of its power under 42 U.S.C. § 1320d-5 (HIPAA's enforcement provision), HHS assessed daily penalties of $1,348,000 for the Encryption Rule violations, $1,500,000 for the 2012 Disclosure Rule violations, and

$1,500,000 for the 2013 Disclosure Rule violations. In total, HHS imposed a civil monetary penalty ("CMP" or "penalty") of $4,348,000.

M.D. Anderson unsuccessfully worked its way through two levels of administrative appeals. Then it petitioned our court for review. *See* 42 U.S.C. § 1320a-7a(e) (authorizing judicial review). After M.D. Anderson filed its petition, the Government conceded that it could not defend its penalty and asked us to reduce it by a factor of 10 to $450,000.

II.

The principal argument in M.D. Anderson's petition is that a state agency is not a "person" covered by HIPAA's enforcement provision. *See* 42 U.S.C. § 1320d-5. For the sake of today's decision, we assume that M.D. Anderson is such a "person" and that the enforcement provision therefore applies. The petition for review nonetheless must be granted for an independent reason: the CMP violates the Administrative Procedure Act ("APA").

A.

The APA directs us to "hold unlawful and set aside" agency actions that are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2); *see Windsor Place v. U.S. Dep't of Health & Hum. Servs.*, 649 F.3d 293, 297 (5th Cir. 2011) (per curiam). To that end, we must "insist that an agency examine the relevant data and articulate a satisfactory explanation for its action." *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 513 (2009) (quotation omitted). Our review is "searching and careful," *Marsh v. Or. Nat. Res. Council*, 490 U.S. 360, 378 (1989) (quotation omitted), and we only consider the reasoning "articulated by the agency itself," *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 50 (1983). *Post hoc* rationalizations offered by the Government's counsel are irrelevant. *See ibid.*

In conducting arbitrary-and-capricious review, we must ensure that the agency did not "entirely fail[] to consider an important aspect of the problem" that it seeks to address. *Id.* at 43. And we must reject "an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise." *Ibid.* Put simply, we must set aside any action premised on reasoning that fails to account for "relevant factors" or evinces "a clear error of judgment." *Marsh*, 490 U.S. at 378 (quotation omitted).

The Supreme Court also has "made clear, however, that a court is not to substitute its judgment for that of the agency and should uphold a decision of less than ideal clarity if the agency's path may reasonably be discerned." *Fox*, 556 U.S. at 513–14 (quotation omitted). "Agencies . . . have expertise and experience in administering their statutes that no court can properly ignore." *Judulang v. Holder*, 565 U.S. 42, 53 (2011). "Fundamentally, the argument about agency expertise is less about the expertise of agencies in interpreting language than it is about the wisdom of according agencies broad flexibility to administer statutory schemes." *Perez v. Mortg. Bankers Ass'n*, 575 U.S. 92, 129 (2015) (Thomas, J., concurring in the judgment).

But in this case, HHS steadfastly refused to interpret the statutes at all. The administrative law judge ("ALJ") began his opinion by emphasizing that he would "not address" any of M.D. Anderson's constitutional or statutory arguments. The ALJ understood his authority to extend only to enforcing HHS's regulations—not to interpreting HIPAA, the HITECH Act, any other statute, or any provision of the U.S. Constitution. As the ALJ put it: "My authority to hear and decide this case rests entirely on a delegation from the Secretary [of HHS]. Nothing in that delegation authorizes me to find that the Secretary's regulations are *ultra vires*."

The ALJ likewise refused to consider whether the multi-million-dollar CMP was arbitrary or capricious. In response to M.D. Anderson's argument that the CMPs in "other instances of ePHI loss . . . were far more lenient than what [the agency] requested in this case," the ALJ concluded: "I do not evaluate penalties based on a comparative standard. There is nothing in the regulations that suggests that I do so."

HHS's Departmental Appeals Board agreed with the ALJ. It held that M.D. Anderson is "free to make its *ultra vires* argument to a court, but we may not invalidate a regulation." And the Board likewise agreed with the ALJ that the agency has no power to review penalties for arbitrariness or capriciousness because "there is nothing in the regulations that suggests that the ALJ evaluate penalties based on a comparative standard."

Thus, with respect to M.D. Anderson's APA arguments—whether the CMP is arbitrary, capricious, or otherwise inconsistent with Congress's statutes—it is impossible for us to substitute our judgment for the agency's. *See Fox*, 556 U.S. at 513–14. That's because the agency itself repeatedly insisted that it was not offering a judgment at all. In accordance with HHS's steadfast insistence in the administrative record, our review of M.D. Anderson's statutory arguments is *de novo*.

Our review of M.D. Anderson's regulatory arguments is also *de novo*. As the Supreme Court recently emphasized, "a court should not afford *Auer* deference unless the regulation is genuinely ambiguous." *Kisor v. Wilkie*, 139 S. Ct. 2400, 2415 (2019).[1] HHS never suggests that its regulations are

[1] The Supreme Court "has often deferred to agencies' reasonable readings of genuinely ambiguous regulations." *Id.* at 2408. It "call[s] that practice *Auer* deference, or sometimes *Seminole Rock* deference, after two cases in which [the Court] employed it." *Ibid.* (citing *Auer v. Robbins*, 519 U.S. 452 (1997); *Bowles v. Seminole Rock & Sand Co.*, 325 U.S. 410 (1945)).

ambiguous, nor does it even cite *Auer*. Therefore, each HHS regulation "just means what it means—and the court must give it effect, as the court would any law." *Ibid.*

B.

The Government's CMP order against M.D. Anderson was arbitrary, capricious, and otherwise unlawful. That's for at least four independent reasons.

1.

Let's start with the Encryption Rule. That Rule provides, in relevant part, that a HIPAA-covered entity must "[i]mplement *a mechanism* to encrypt and decrypt electronic protected health information." 45 C.F.R. § 164.312(a)(2)(iv) (emphasis added).[2] It is undisputed that M.D. Anderson implemented "a mechanism." For example, M.D. Anderson's "Information Resources Acceptable Use Agreement and User Acknowledgement for Employees" specified: "If confidential or protected MDACC data is stored on portable computing devices, *it must be encrypted* and backed up to a network server for recovery in the event of a disaster or loss of information." M.D. Anderson furnished its employees an "IronKey" to encrypt and decrypt mobile devices and trained its employees on how to use it. M.D. Anderson also implemented a mechanism to encrypt emails. And M.D. Anderson implemented various other mechanisms for file-level encryption in

[2] The parties agree that the Encryption Rule does not require *all* entities to adopt such "a mechanism." Encryption is a so-called "addressable" requirement, which means that a covered entity can "address" it by explaining why it's not "reasonable and appropriate" under that covered entity's particular circumstances. *See* 45 C.F.R. § 164.306(d). It's undisputed that M.D. Anderson thought an encryption mechanism was reasonable and appropriate, and that it attempted to adopt one that satisfied the Encryption Rule. Therefore, for purposes of this opinion, we ignore the "addressability" carveout to the Encryption Rule.

its ClinicStation software. Petitioner plainly implemented "a mechanism" to encrypt ePHI.

The dispute in this case is whether M.D. Anderson should've done more—either to implement a different mechanism or to better implement its chosen mechanism. The Government adamantly argues yes. First, HHS argues that M.D. Anderson's internal documents show that Petitioner wanted to strengthen its mechanisms for protecting ePHI. But it's plainly irrational to say that M.D. Anderson's desire to do more in the future means that in the past it "failed to encrypt patient data on portable media *at all*." Red Br. 48 (emphasis by HHS).

Second, the Government argues that the stolen laptop and the two lost USB drives were not encrypted at all. That appears undisputed. But that does not mean M.D. Anderson failed to implement "a mechanism" to encrypt ePHI. It means only that three employees failed to abide by the encryption mechanism, or that M.D. Anderson did not enforce that mechanism rigorously enough. And nothing in HHS's regulation says that a covered entity's failure to encrypt three devices means that it never implemented "a mechanism" to encrypt anything at all.

For example, imagine that a covered entity has a million USB drives. It pays millions of dollars for military-grade encryption of those drives, with the expectation that they would be impervious to the most sophisticated computer hackers on earth. Then the covered entity puts ePHI on the drives. What happens if a new hacker nonetheless decrypts three of them? Or what if someone in the factory accidentally fails to encrypt three USB drives, and they get stolen? Under the Government's theory, the covered entity violated the Encryption Rule because the decrypted or unencrypted devices prove *res ipsa* it could've done more. As the ALJ understood the Encryption Rule, it

"require[s] covered entities to assure that all systems containing ePHI be inaccessible to unauthorized users." Period. Full stop. No exceptions.[3]

But that's not the regulation HHS wrote. The regulation requires *only* "a mechanism" for encryption. It does not require a covered entity to warrant that its mechanism provides bulletproof protection of "all systems containing ePHI." Nor does it require covered entities to warrant that all ePHI is always and everywhere "inaccessible to unauthorized users." Nor does the regulation prohibit a covered entity from creating "a mechanism" by directing its employees to sign an Acceptable Use Agreement that requires encryption of portable devices. Nor does it say that providing employees an IronKey is insufficient to create a compliant mechanism. Nor does it say anything about how effective a mechanism must be, how universally it must be enforced, or how impervious to human error or hacker malfeasance it must be. The regulation simply says "a mechanism." M.D. Anderson undisputedly had "a mechanism," even if it could've or should've had a better one. So M.D. Anderson satisfied HHS's regulatory requirement, even if the Government now wishes it had written a different one.

---

[3] It's no answer to say, as the Government does, that there's a significant difference between M.D. Anderson and the hypothetical herculean covered entity that pays millions of dollars for military-grade encryption on some of its portable devices. As M.D. Anderson points out, there's ample evidence in the administrative record that Petitioner spent considerable money and energy protecting ePHI and implementing improvements to its ePHI protections. And in all events, the Encryption Rule does not contain a Herculean-Efforts Exception that protects one covered entity and not another based on how hard they try to encrypt ePHI. As relevant here, *see supra* note 2, the Rule requires *all* covered entities to establish "a mechanism." And a covered entity either satisfies that requirement by creating "a mechanism" (as M.D. Anderson argues) or it faces strict liability for creating no mechanism at all if three of its devices are unencrypted or decrypted (as HHS argues). As explained above, we agree with M.D. Anderson. If HHS wants to police just how herculean a covered entity must be in encrypting ePHI, the Government can propose a rule to that effect and attempt to square it with the statutes Congress enacted.

2.

Next consider the Disclosure Rule. With exceptions not relevant here, that Rule prohibits a covered entity from "disclos[ing]" ePHI. 45 C.F.R. § 164.502(a). And the Rule defines "disclosure" to "mean[] the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." *Id.* § 160.103. The ALJ seized on the word "release" and concluded that a covered entity violates the Disclosure Rule whenever it loses control of ePHI—regardless of whether anyone outside of M.D. Anderson accesses it.

That interpretation departs from the regulation HHS wrote in at least three ways. First, each verb HHS uses to define "disclosure"—release, transfer, provide, and divulge—suggests an affirmative act of disclosure, not a passive loss of information. One does not ordinarily "transfer" or "provide" something as a sideline observer but as an active participant. The ALJ recognized as much when he defined "release" as "*the act* of setting something free." But then he made the arbitrary jump to the conclusion that "*any* loss of ePHI is a 'release,'" even if the covered entity did not act to set free anything. It defies reason to say an entity affirmatively acts to disclose information when someone steals it. That is not how HHS defined "disclosure" in the regulation. So HHS may not define it that way in an adjudication.[4]

[4] That is not to say that a covered entity must *knowingly* act to disclose ePHI to violate HIPAA. To the contrary, Congress specified penalties for unknowing violations. *See* 42 U.S.C. § 1320d-5(a)(1)(A) (prescribing penalties where the entity "did not know" it committed a violation); *cf. infra* at 12 (discussing statutory penalties for "reasonable cause" and "willful neglect" violations). One can affirmatively disclose something to someone outside a covered entity and do so unknowingly—say, by emailing protected information to the wrong "John Doe."

Second, each of the regulation's disclosure-defining verbs is transitive. The Disclosure Rule prohibits the release, transfer, provision, and divulging of a particular object—namely, "information." 45 C.F.R. § 160.103. And the Government nowhere explains how "information" can be released, transferred, provided, or divulged without *someone* to receive it and hence be informed by it. To the contrary, the regulation appears to define "disclosure" in accordance with its ordinary meaning, which requires information to be "made known" to someone. *See* WEBSTER'S NEW INTERNATIONAL DICTIONARY 743 (2d ed. 1934; 1950). HHS never explains how someone could "disclose" a secret without actually making it known to someone. Nor can we imagine a way.

Third, the Disclosure Rule does not prohibit disclosure to just *any* someone. The ePHI must be disclosed to someone "outside" of the covered entity. 45 C.F.R. § 160.103. The Government's loss-of-control standard means that a covered entity can be liable under the Disclosure Rule if one employee shares or steals another employee's laptop. But that interpretation renders the word "outside" in § 160.103 meaningless surplusage. *See Nat'l Ass'n of Home Builders v. Defs. of Wildlife*, 551 U.S. 644, 668–69 (2007) (rejecting an interpretation that "would render the regulation entirely superfluous"). We therefore refuse to interpret § 160.103 to mean that HHS can prove that M.D. Anderson "disclosed" ePHI without proving that someone "outside" the entity received it. And the Government concedes it cannot meet that standard.

The Government's principal response is that it will be difficult for HHS to enforce the Disclosure Rule if it must show that ePHI was disclosed to someone, and harder still if it must show that ePHI was disclosed "outside" of the covered entity. Maybe so, maybe not. But that's precisely the sort of policy argument that HHS could vet in a rulemaking proceeding.

It's not an acceptable basis for urging us to transmogrify the regulation HHS wrote into a broader one.

3.

Third, one of the most remarkable aspects of the ALJ's order is its insistence that the Government can arbitrarily and capriciously enforce the CMP rules against some covered entities and not others. The ALJ insisted that "I do not evaluate penalties based on a comparative standard. There is nothing in the [HHS] regulations that suggests that I do so." The Departmental Appeals Board agreed with the ALJ's legal reasoning.

It is a bedrock principle of administrative law that an agency must "treat like cases alike." 32 CHARLES ALAN WRIGHT & CHARLES H. KOCH, FEDERAL PRACTICE AND PROCEDURE § 8248, at 431 (2006); *see also Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 981 (2005) ("Unexplained inconsistency is . . . a reason for holding [agency action] to be . . . arbitrary and capricious . . . ."); *Burlington N. & Santa Fe Ry. Co. v. Surface Transp. Bd.*, 403 F.3d 771, 776 (D.C. Cir. 2005) ("An agency must provide an adequate explanation to justify treating similarly situated parties differently."); WRIGHT & KOCH, *supra*, § 8248, at 431 ("General principles of administrative law hold that an agency must be consistent . . . ."). This principle is an outgrowth of the old adage from *State Farm* that "an agency changing its course must supply a reasoned analysis." 463 U.S. at 57 (quotation omitted); *accord Fox*, 556 U.S. at 515 ("[T]he requirement that an agency provide reasoned explanation for its action . . . ordinarily demand[s] that it display awareness that it is changing position. . . . [T]he agency must show that there are good reasons for the new [position]." (emphasis omitted) (citation omitted)); *Jupiter Energy Corp. v. FERC*, 407 F.3d 346, 349 (5th Cir. 2005) (agency action is arbitrary and capricious when it fails to "supply a reasoned analysis for any departure from

other agency decisions" (quotation omitted)); *Comcast Corp. v. FCC*, 526 F.3d 763, 769 (D.C. Cir. 2008) ("[A]n agency's unexplained departure from precedent must be overturned as arbitrary and capricious.").

But in this case, M.D. Anderson proffered examples of other covered entities that violated the Government's understanding of the Encryption Rule and faced zero financial penalties. For example, a Cedars-Sinai employee lost an unencrypted laptop containing ePHI for more than 33,000 patients in a burglary. HHS investigated and imposed no penalty at all. The Government has offered no reasoned justification for imposing zero penalty on one covered entity and a multi-million-dollar penalty on another.

The Government's only response is that it evaluates each case on its individual facts. As it must. But an administrative agency cannot hide behind the fact-intensive nature of penalty adjudications to ignore irrational distinctions between like cases. *See LeMoyne-Owen Coll. v. NLRB*, 357 F.3d 55, 61 (D.C. Cir. 2004) ("[W]here, as here, a party makes a significant showing that analogous cases have been decided differently, the agency must do more than simply ignore that argument."). Were it otherwise, an agency could give free passes to its friends and hammer its enemies—while also maintaining that its decisions are judicially unreviewable because each case is unique. Suffice it to say the APA prohibits that approach.

4.

Fourth, the penalty amounts. The ALJ found that M.D. Anderson's violations of the Encryption Rule and the Disclosure Rule were attributable to "reasonable cause" and not "willful neglect." 42 U.S.C. § 1320d-5(a)(1)(B). For such "reasonable cause" violations, Congress specified that "the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $100,000." *Id.* § 1320d-5(a)(3)(B). The ALJ and the Departmental Appeals

Board nevertheless determined that the per-year statutory cap was *$1,500,000*. Then the agency determined that M.D. Anderson owed $1,348,000 over the calendar years 2011, 2012, and 2013 for violating the Encryption Rule and $3,000,000 for calendar years 2012 and 2013 for violating the Disclosure Rule.

Again, that's arbitrary, capricious, and contrary to law. Congress specified that the per-year cap for all reasonable-cause violations is $100,000—not $1,500,000. *See* 42 U.S.C. § 1320d-5(a)(3)(B); *cf. Util. Air Regul. Grp. v. EPA*, 573 U.S. 302, 328 (2014) (holding agency has no power to rewrite numerical thresholds imposed by Congress). Two months after the Departmental Appeals Board's decision in this case, HHS conceded that it had misinterpreted the statutory caps. And it published a "Notice of Enforcement Discretion Regarding HIPAA Civil Money Penalties" to explain its *mea culpa*. *See* 84 Fed. Reg. 18,151, 18,153 (Apr. 30, 2019). In its *mea culpa*, HHS said that "[u]pon further review of the statute by the HHS Office of the General Counsel," it would exercise "enforcement discretion" to follow the statutory caps in 42 U.S.C. § 1320d-5(a)(3)(B). *Ibid.* (citing *Heckler v. Chaney*, 470 U.S. 821, 831 (1985)).[5]

[5] Section 1320d-5(a)(1)(B) says that reasonable-cause violations shall incur "a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(B) but not to exceed the amount described in paragraph (3)(D)." Paragraph (3)(B) in turn imposes a per-violation amount of $1,000, and paragraph (3)(D) imposes a per-violation amount of $50,000. It is quite obvious from that statutory text that each reasonable-cause violation can be penalized from $1,000 to $50,000—but the total of all reasonable-cause violations for a calendar year cannot exceed $100,000. In the ALJ's CMP order and the Departmental Appeals Board's decision, however, HHS said each reasonable-cause violation can be penalized from $1,000 to $50,000 up to the calendar-year limit of *$1,500,000* that applies to *uncorrected willful-neglect violations*. *See* 42 U.S.C. § 1320d-5(a)(1)(C)(ii). In addition to nonsensically conflating the fault levels specified by Congress, HHS's interpretation rendered meaningless surplusage the statutory cap for

We take the opportunity to reiterate what we've said before: neither "enforcement discretion" nor *Heckler v. Chaney* empowers an agency to disregard Congress's statutes. *See Texas v. United States*, 809 F.3d 134, 152 n.34 (5th Cir. 2015) (citing *Heckler*, 470 U.S. at 831), *aff'd by an equally divided Court*, 136 S. Ct. 2271 (2016) (per curiam). And the fact that HHS later recognized its error in a notice of "enforcement discretion" does nothing to change the text of the regulations HHS promulgated through notice and comment. Nor does it cure the erroneous premises of the decisions by the ALJ and the Departmental Appeals Board.

Those erroneous premises are particularly problematic because they tainted other parts of HHS's decision. For example, HHS's own regulations require it to consider the following factors (among others) in assessing a CMP:

> (1) Whether the violation caused physical harm;
>
> (2) Whether the violation resulted in financial harm;
>
> (3) Whether the violation resulted in harm to an individual's reputation; and
>
> (4) Whether the violation hindered an individual's ability to obtain health care.

45 C.F.R. § 160.408(b). It's undisputed that HHS can prove none of these. But the ALJ justified ignoring them because "the penalties that I determine to impose are but a small fraction of the maximum penalties that are

---

reasonable-cause violations. *But see Corley v. United States*, 556 U.S. 303, 314 (2009) (emphasizing "one of the most basic interpretive canons, that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant" (quotation omitted)). The indefensibility of its prior interpretation presumably explains HHS's notice of "enforcement discretion."

permitted by regulation"—a regulation that HHS now concedes in its "enforcement discretion" is unlawful.

* * *

The Government has offered no lawful basis for its civil monetary penalties against M.D. Anderson. The petition for review is GRANTED. The CMP order is VACATED. And the matter is REMANDED for further proceedings consistent with this opinion.