UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	§	
	§	**Criminal No. 24-CR-00298**
V.	§	
	§	
EITHAN HAIM	§	

DEFENDANT'S MOTION TO DISMISS AND MOTION TO STRIKE

The defendant, Dr. Eithan Haim, moves for the Court to dismiss the superseding indictment and the case with prejudice because the indictment is invalid on its face and cannot be fixed. If the Court determines that some allegations and counts may survive, Dr. Haim moves for the Court to strike the remainder.

When the government indicted Dr. Haim for felony violations of HIPAA, it was charting new territory. Very few criminal HIPAA cases have ever been litigated, even fewer under the felony provisions. None have addressed the scope or validity of the two basic means of committing the offense: 1) acting without authorization and 2) violating HIPAA regulations. Yet the government was not cautious. The first indictment contained significant factual and legal errors. When the government brought the superseding indictment, it failed to fix those errors and introduced new ones of even more gravity. These errors cannot be fixed with another amendment.

Both means of committing the crimes alleged are invalid. The thin reed upon which the government hangs its case—that Dr. Haim acted without authorization—collapses because TCH gave him access to its system. HIPAA privacy regulations also cannot serve as a basis for liability because no violation of those can trigger the HIPAA crime of obtaining health information. Indeed, no jury instruction is possible. And even if those fatal errors could be fixed, the Court must nevertheless strike material from or dismiss the superseding indictment because it contains material drafting errors; it cites a non-existent provision and a non-existent crime.

There is no basis for proceeding to trial. Even if all the allegations were proven, that would not establish criminal liability. The legal errors would also make a trial entirely unmanageable. A trial would proceed on theories requiring voluminous evidence under vague standards. It would be impracticable to prevent the jury's consideration of evidence supporting one theory for the other, so if any were held unlawful on appeal, the difficult trial work would be mooted. This case is the ideal vehicle for dismissal and the clarification of any legal theory on appeal.[1]

SUMMARY

The superseding indictment must be dismissed because there is no HIPAA crime here. Neither means of committing the crime alleged are viable.

[1] *See* James M. Burnham, *Why Don't Courts Dismiss Indictments?*, 18 GREEN BAG 2d 347 (2015).

The Supreme Court itself has already shot down the first means, obtaining health information "without authorization." In 2021 it held, for an analogous statute, that the "without authorization" inquiry is a "gates-up-or-down" test that can never be satisfied by simply violating an employer's access policies. Because the superseding indictment effectively acknowledges that the hospital authorized Dr. Haim to access medical records and the government cannot dispute it, "without authorization" cannot serve as the basis for a conviction.

For the second means, violating HIPAA regulations, the government fails to allege a violation. The allegation in every count that Dr. Haim obtained health information "for a reason other than those permitted by" the provisions of HIPAA cites a non-existent statutory provision, and there is no correct statutory provision to cite. Similarly, Counts 2–4 duplicitously charge obtaining "and/or" using health information, even though "using" it is not a crime.

These fatal drafting errors reveal a fundamental legal error. Violating HIPAA privacy regulations can *never* serve as a basis for the crime of "obtaining" health information. The regulations themselves do not prohibit any manner of "obtaining" information, only using it. Congress also failed to incorporate those regulations into the criminal HIPAA provision. And if they were so incorporated, that would create serious constitutional problems that require avoidance of such an interpretation.

These legal infirmities in the superseding indictment go to the core of the government's case. The case cannot proceed to trial on the superseding indictment or any further amended one. It should be dismissed.

BACKGROUND

I. Statutory and Regulatory Background

This case concerns the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Pub. L. No. 104–191, 110 Stat 1936 (1996). Through HIPAA, Congress "addressed the opportunities and challenges presented by the health care industry's increasing use of and reliance on electronic technology." Standards for Privacy of Individually Identifiable Health Information in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 64 Fed. Reg. 59918, 59920 (Nov. 3, 1999).

The original HIPAA statute had civil and criminal penalties. Many of the specifics later changed, but it has always criminally punished "[a] person who knowingly and in violation of this part . . . obtains individually identifiable health information" (IIHI) and civilly fined "any person who violates a provision of this part." *See* HIPAA § 262(a); 42 U.S.C. § 1320d–5, 1320d–6. The critical term "this part" refers to "Part C—Administrative Simplification," added at the end of Title XI of the Social Security Act according to Section 262(a) of HIPAA. Section 262 sets out the provisions that were codified at Sections 1320d through 1320d–8 of Title 42.

Some of those provisions specified that the Department of Health and Human Services (HHS) would promulgate regulations. What became Sections 1320d–1 and 1320d–2 provided that HHS would promulgate "standards to enable electronic exchange," other transaction-focused standards, and "security standards." But one particular set of regulations, those setting privacy standards, were authorized in a separate section of HIPAA. This reflects the convoluted history of the legislative text. The Department of Health and Human Services summarized it 25 years ago:

> In section 262, Congress recognized and sought to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords. Thus, section 262 directs HHS to issue standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit electronically in connection with such transactions. HHS proposed such standards in a series of Notices of Proposed Rulemaking (NPRM) . . . . At the same time, Congress recognized the challenges to the confidentiality of health information presented by the advances in electronic technology and communication. Section 262 thus also directs HHS to develop standards to protect the security, including the confidentiality and integrity, of such information. HHS issued an NPRM proposing security standards on August 12, 1998 (63 FR 43242).
>
> Congress has recognized that privacy standards must accompany the electronic data interchange standards and that the increased ease of transmitting and sharing individually identifiable health information must be accompanied by an increase in the privacy and confidentiality. In fact, a significant portion of the first Administrative Simplification section that was debated on the floor of the Senate in 1994 (as part of the Health Security Act) was made up of privacy provision. Although the requirement for the issuance of concomitant privacy standards remained as part of the bill passed by the House of Representatives, in conference the requirement for privacy standards was removed from

> the standard-setting authority of title XI (section 1173 of the Act) and placed in a separate section of HIPAA, section 264. Subsection (b) of section 264 required the Secretary of HHS to develop and submit to the Congress recommendations for:
>
> (1) The rights that an individual who is a subject of individually identifiable health information should have.
> (2) The procedures that should be established for the exercise of such rights.
> (3) The uses and disclosures of such information that should be authorized or required.
>
> The Secretary's Recommendations were submitted to the Congress on September 11, 1997 . . . Section 264(c)(1) provides that: "If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by (August 21, 1999), the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than (February 21, 2000). Such regulations shall address at least the subjects described in subsection (b)."

64 Fed. Reg. at 59920.

Congress did not succeed in passing privacy standards, so HHS published a notice of proposed rulemaking for the "Privacy Rule" in November 1999 and a final rule in December 2000. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82470 (Dec. 28, 2000).

The HIPAA statute states that any standard adopted under Part C will apply only to health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with certain transactions. 42 U.S.C. § 1320d–1(a). The Privacy Rule defines "covered entity"

the same way, and this definition applies to all of HHS's HIPAA regulations (including rules beyond the Privacy Rule). 65 Fed. Reg. at 82799. HHS relied on 42 U.S.C. § 1320d–2(a)(1) to promulgate that definition. *See id.*

Because HIPAA regulations apply only to "covered entities," a person can obtain IIHI "in violation of" Part C only if he or she is a covered entity. The U.S. Department of Justice Office of Legal Counsel (OLC) reached this simple conclusion with much supporting analysis. *See* Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6, 29 U.S. Op. Off. Legal Counsel 76 (June 1, 2005) ("OLC Memo").

Congress was not pleased with this result. In the American Recovery and Reinvestment Act of 2009, Pub. L. 111–5, 123 Stat 115 (2009), Congress ensured that liability would extend beyond covered entities. To the end of the criminal provision, Congress added:

> a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1180(b)(3)) and the individual obtained or disclosed such information <u>without authorization</u>.

Id. § 13409 (amending the provision codified at 42 U.S.C. § 1320d–6(a)) (emphasis added).

The Conference Report made the purpose of this addition clear. It recognizes that the "Office of Legal Counsel (OLC) addressed which persons may be

prosecuted under HIPAA and concluded that only a covered entity could be criminally liable." H. Rept. No. 111-16, at 500 (2009) (Conference Report). In response, the "House bill clarifies that criminal penalties for wrongful disclosure of [protected health information] apply to individuals who without authorization obtain or disclose such information maintained by a covered entity, whether they are employees or not," and the Senate bill agreed. *Id.* (emphasis added).

II. The Indictments

The government obtained an indictment in May 2024 charging Dr. Haim with four counts of violating the criminal HIPAA provision by "knowingly and without authorization, and for a reason other than those permitted by Title 42, United States Code, Chapter 7, Subchapter XL, Part C (provisions of HIPAA)" performing certain acts. Indictment, Dkt. No. 1, at 4–5. Count 1 charged that he "obtained" IIHI, and Counts 2–4 charged that he "did obtain and/or wrongfully disclose" IIHI. In October 2024, the government obtained a superseding indictment. While it revised or removed certain factual allegations, the means of committing the base offense specified in each count remains the same. But for Counts 2–4, the charge changed to being that Dr. Haim "did obtain and/or use" IIHI. Superseding Indictment, Dkt. No. 76 at 4.

LEGAL STANDARD

The superseding indictment contains multiple types of legal errors, and some are amenable to multiple remedies.

Whether an indictment should be dismissed for insufficiency "by pretrial motion is by-and-large contingent upon whether the infirmity in the prosecution is essentially one of law or involves determinations of fact. . . . If a question of law is involved, then consideration of the motion is generally proper." *United States v. Fontenot*, 665 F.3d 640, 644 (5th Cir. 2011) (quoting *United States v. Flores*, 404 F.3d 320, 324 (5th Cir. 2005)). "In reviewing a challenge to an indictment alleging that it fails to state an offense, the court is required to take the allegations of the indictment as true and to determine whether an offense has been stated." *United States v. Crow*, 164 F.3d 229, 234 (5th Cir. 1999).

A duplicitous indictment alleges "two or more distinct and separate offenses" in a single count. *United States v. Caldwell*, 302 F.3d 399, 407 (5th Cir. 2002). The court asks "whether [the indictment] can be read to charge only one violation in each count." *Id.* (quoting *United States v. Sharpe*, 193 F.3d 852, 866 (5th Cir. 1999)). If an indictment is duplicitous and prejudice results, the conviction may be reversed. *United States v. Baytank (Houston), Inc.,* 934 F.2d 599, 608 (5th Cir. 1991).

Allegations in an indictment that are unnecessary to prove the crime charged are surplusage. *United States v. Miller,* 471 U.S. 130, 136–37 (1985). Surplusage

may not be readily disregarded where the charge is "materially broadened." *See United States v. Trice*, 823 F.2d 80, 89 n.8 (5th Cir. 1987). Material is unduly prejudicial and must be struck if the language "serve[s] only to inflame the jury, confuse[s] the issues, and blur[s] the elements necessary for conviction." *United States v. Bullock*, 451 F.2d 884, 888 (5th Cir. 1971). A court may strike as surplusage any "[i]ndirect expressions, implied allegations, argumentative statements, and uncertainty due to generalizations in language." *United States v. Williams*, 203 F.2d 572, 574 (5th Cir. 1953).

ARGUMENT

The superseding indictment relies on legal theories for both means of committing the base offense that are fundamentally invalid. But it also contains simple yet fatal drafting errors that require action. Because the problems cannot be fixed by amendment, the superseding indictment and case should be dismissed.

I. No indictment can rely on Dr. Haim's obtaining records "without authorization."

The criminal provision treats obtaining IIHI as a violation "if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d–6(a). The text of the provision makes clear that this means of committing the base HIPAA offense is

separate from any regulations (discussed below).[2] But the statute itself provides no further definition or guidance. It appears that no case has interpreted this phrase, and it is unclear whether any prosecution has ever relied on it. The text straightforwardly means that the covered entity maintaining the information must provide "authorization." But it gives no further indication of what kind of authorization is meant.

The very same phrase, though, appears in the Computer Fraud and Abuse Act (CFAA), which preceded HIPAA. Like HIPAA, which is generally concerned with health information transmitted electronically, *see* 42 U.S.C. § 1320d–1(a), the CFAA protects information held in almost any computer, *see* 18 U.S.C. § 1030(a)(2). But unlike HIPAA, the CFAA not only punishes access "without authorization" but also anyone who "exceeds authorized access" and thereby obtains information. *Id.* These two phrases caused a great deal of confusion in the lower courts for decades, until the Supreme Court finally resolved their meanings in *Van Buren v. United States*, 593 U.S. 374 (2021).

In that case, a police sergeant misused a law enforcement database; although he had legitimate access, he searched for another person's information for "an improper purpose," which he knew violated department policy. *Id.* at 380. The

[2] Authorization in the regulations is by the patient—unlike in this statutory standard, many uses and disclosures properly occur without authorization. *See, e.g.*, 45 C.F.R. § 164.512.

Government told the jury that his actions "'violated the CFAA concept' against 'using' a computer network in a way contrary to 'what your job or policy prohibits.'" *Id.*

The Supreme Court disagreed. It held that the CFAA "does not cover those who . . . have improper motives for obtaining information that is otherwise available to them." *Id.* at 378. The Court focused on resolving the meaning of "exceeds authorized access" and determined that it applies only to those who obtain information from areas to which their computer access does not extend (so-called "inside hackers"), not those who misuse access that they otherwise have to those areas. *Id.* at 381, 389. But in doing so, the Court looked at the meaning of "without authorization." There, both the government and defendant agreed that "without authorization" is a "gates-up-or-down inquiry—one either can or cannot access a computer system," and so it is satisfied only when access occurs "without any permission at all" (an "outside hacker"). *Id.* at 389–90. Specifically, the government did not read "without authorization" "to incorporate purpose-based limits contained in contracts and workplace policies." *Id.*

HIPAA's "without authorization" clause should logically function the same way. If the covered entity that maintains the IIHI grants someone access to any part of its electronic medical records system, the gates are up, and any activity in the system is not "without authorization."

This understanding also makes sense of the legislative history. Per the OLC memo, HIPAA criminal liability would apply to health care providers (who would be authorized to access the EMR system and therefore be bound by any legitimate regulations on covered entities) and the leadership of hospitals, but it would not necessarily apply to other low-level employees or to non-employees—including those who purloin IIHI in even the most egregious circumstances. *See* OLC Memo. The lacuna was addressed by the "without authorization" provision Congress added. This explains why the provision covers "a person (including an employee or other individual)" and why the Conference Report states that it would "apply to individuals who without authorization obtain or disclose such information maintained by a covered entity, whether they are employees or not." H. Rept. No. 111-16, at 500. The "without authorization" provision adds liability to those who obtain information or disclose IIHI but have no authorization to do even that type of task. Someone need not "break in" (physically or digitally) to a data-storage facility to access IIHI "without authorization," but those granted access cannot access the relevant data "without authorization." In other words, janitors who access an unlocked EMR terminal and people who scam their way into a hospital data center as a deliveryman to copy records would violate this HIPAA provision, but not doctors to whom the hospital gives login credentials.

A contrary approach that makes authorization hinge on hospital policies, terms of use, or the purpose for obtaining IIHI would create chaos. Congress did not even add the more limited concept of "exceeds authorized access" to HIPAA, so its intent is doubly clear that policies do not matter for the inquiry. But the *Van Buren* Court also recognized the practical implications of such an approach in CFAA—it would "attach criminal penalties to a breathtaking amount of commonplace computer activity." 593 U.S. at 393. Indeed, the lower courts struggled for decades over whether and which policy-based violations create liability, and many recognized the approach is simply unworkable and causes arbitrary enforcement.[3] Even the Fifth Circuit has gotten it wrong.[4] *See United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010) (following an "intended-use analysis"), *abrogated by Van Buren*, 593 U.S. 374.[5]

[3] *See, e.g.*, Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 Harv. J.L. & Tech. 479, 481–82 (2019) ("Thousands of pages of jurists' opinions and scholars' law review articles have pointed out the CFAA's doctrinal limitations and struggled to interpret the statute's core provisions. The CFAA has generated heated policy debate, circuit splits, and much public outcry, but, alas, none of the attempted solutions have successfully remedied its flaws over thirty years' time."); Melanie Assad, *Van Buren v. United States: An Employer Defeat or Hackers' Victory-or Something in Between?*, 21 UIC Rev. Intell. Prop. L. 166, 170–71 (2022).

[4] The Supreme Court recently reversed another conviction under a statute that criminalizes someone who uses, "without lawful authority," a means of identification of another person during and in relation to health care fraud in part because the government's view of that term was too capacious. *Dubin v. United States*, 599 U.S. 110, 124 (2023).

[5] If the U.S. Attorney's Office decides to take a view of the meaning of the phrase contrary to that of the Solicitor General in *Van Buren*, the defense will gladly expand on these issues and their implications for trial. For some additional questions, see Orin S. Kerr, *Focusing the CFAA in* Van Buren, 2021 Sup. Ct. Rev. 155, 179 (2021).

Here, the many problems raised by such an approach would include:

(1) What happens when the policies are narrower than HIPAA and restrict actions that HIPAA allows (such as disclosures to law enforcement about a hospital's misconduct)?

(2) Who has actual or apparent authority to explicitly or implicitly amend hospital polices: an attending physician? a hospital bureaucrat?

(3) How do the policies apply to non-employee physicians (such as Baylor College of Medicine residents on other rotations), and what kind of notice (if any) would the hospital have to provide of policy changes (including unwritten ones) to subject someone to criminal liability for an infraction?

These intensely factual questions will be matched by the excruciatingly specific evidence that would be adduced at a trial on these issues. They suffice to make clear that this approach simply does not work.

The superseding indictment does not—and cannot—allege that Dr. Haim had no permission to be in TCH's electronic medical records system. Instead, it states that he contacted TCH to re-activate his login credentials (which had expired) and that he later had "login activity" by which he accessed records, implying that TCH re-activated his login credentials. *See* Superseding Indictment ¶¶ 9–10. While the government has been loath to admit, as TCH itself already has, *see* Dkt. No. 84 at 3, that Dr. Haim's access was "authorized" by TCH, it has never disputed that TCH

granted the access to Dr. Haim that form the basis of the charges. Instead, it has implicitly admitted that it did. *See* Dkt. No. 33 at 4 (noting that Dr. Haim "successfully renew[ed] his login credentials" and not suggesting that this occurred from hacking).

Because TCH granted Dr. Haim access, his obtaining any IIHI was not "without authorization." There is no reason to submit this question to a jury—and thus the government's entire theory of the case collapses.

II. Fatal drafting errors in the superseding indictment require its dismissal or the striking of significant allegations and point to the lack of any liability under HIPAA regulations.

There are many drafting errors in the superseding indictment. Two in particular require immediate action, but they also point to much larger problems that prevent the government from relying on the second means, violation of HIPAA privacy regulations, to prove a crime.

First, the superseding indictment cites a nonexistent statutory provision. All four counts charge that Dr. Haim obtained IIHI "for a reason other than those permitted by Title 42, United States Code, Chapter 7, Subchapter XL, Part C (provisions of HIPAA)." Dkt. No. 76 at 4. But there is no "Subchapter XL" in Chapter 7 of Title 42. The government may be referring to Subchapter XI, in which the criminal provision is found. The lengthy phrase may represent the government's attempt to track the criminal provision's element of "in violation of this part." But

"this part" in the statute refers to Part C of Title XI of the Social Security Act, not Part C of the Code. In any event, that gives no notice of how any "reason" is invalid; neither Part Cs enumerate the valid reasons for obtaining IIHI.

That vagueness means that the government's error both misleads and prejudices. Fed. R. Crim. Proc. 7(c)(2). But to cut to the chase, the defense recognizes that in other prosecutions, the government has typically meant to refer to the Privacy Rule with similar (though correct) U.S. Code references. The government's pretrial motions and opposition to Dr. Haim's motion for a bill of particulars both rely on the Privacy Rule. Dkt. No. 33 at 2–3; 10–11; Dtk. No. 43 at 4–5. But if that is what the government intends, there is no crime. Violations of the Privacy Rule cannot support criminal liability here, as discussed below.

Second, and relatedly, the superseding indictment has amended language in Counts 2–4 that results in an unlawful duplicitous charge, or at least prejudicial surplusage. They now allege that Dr. Haim "did obtain and/or use" IIHI. Federal prosecutors generally charge even disjunctive statutes conjunctively to avoid problems with duplicity. Here, the disjunctive "or" creates duplicity because it brings together two offenses. One is the offense of obtaining IIHI under Section 1320d–6(a). The second is the nonexistent offense—certainly not found in that same section—of "using" IIHI. Granted, the most significant felony punishment also requires an "intent to sell, transfer, or use." 42 U.S.C. 1320d–6(b)(3). But the statute

criminalizes only the action of obtaining the IIHI unlawfully, while the charged crime as written can be found solely by "use." This foreshadows the government's confusion over the Privacy Rule, which has only "use" and not "obtain," but for now that distinction is enough to demonstrate that the superseding indictment presents a non-crime as a crime.

The "use" offense also represents prejudicial surplusage. Having a means of committing the charged crime that is not illegal will certainly confuse the jury and blur the elements. *Bullock*, 451 F.2d at 888. But the charge also suggests that Dr. Haim's alleged use of the information to blow the whistle was criminal even though the government has not charged his disclosure. This will inflame the jury and prejudice Dr. Haim even if the jury instructions prescribe that only obtaining IIHI can constitute a crime.

These two errors are significant enough on their own to warrant dismissal of the superseding indictment or striking most of it. Yet the government cannot fix these problems because there are more fundamental errors with the means of committing the crimes to which they point.

III. Violations of the Privacy Rule do not create a crime based on the access alleged here.

While the indictment does not expressly charge Dr. Haim with violating the Privacy Rule as the means of violating "this part" (of Title XI of the Social Security Act), its filings so far (*see* Dkt. No. 33 at 2–3; 10–11; Dtk. No. 43 at 4–5), the

government's practice in such cases, and the nature of the allegations set that up. The government's failure to clearly articulate the means of violating "this part" are no accident. Drawing a clean line from specific provisions of the Privacy Rule to a violation of the criminal provision is impossible, especially for the charges here. The Privacy Rule simply does not regulate obtaining IIHI, so a violation of that cannot support criminal liability. But the Privacy Rule is also not part of "this part" either. And investing the Privacy Rule with criminal power would be unconstitutional.

A. The Privacy Rule has no prohibitions on obtaining information.

A violation of the Privacy Rule cannot support a conviction for obtaining IIHI under the criminal HIPAA provision because there is a fundamental mismatch in the terms each uses.

The government charges that Dr. Haim did "obtain" IIHI. Black's Law Dictionary defines "obtain" unremarkably as "[t]o bring into one's own possession; to procure, esp. through effort." Black's Law Dictionary (12th ed. 2024).

The Privacy Rule, however, makes no mention of "obtain." Instead, it speaks throughout of "uses and disclosures." *See, e.g.*, 45 CFR § 164.502. "Use" is defined as, "with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information." 45 C.F.R. § 160.103.

"Use" is defined by the Privacy Rule in a way that does not overlap at all with "obtain." Thus, when someone obtains IIHI, he does not violate the Privacy Rule by that act. And if he transgresses the Privacy Rule by using the information (such as by "examination" of it), he has already completed obtaining it. Likewise, any disclosure occurs after the IIHI is obtained. So no violation of the Privacy Rule can support a charge premised on obtaining IIHI.

This result makes sense, at least for Congress and HHS. When Congress gave HHS its charge to draft the Privacy Rule in HIPAA Section 264, it mentioned only "uses and disclosures of [IIHI] that should be authorized or required." HHS followed that charge precisely. In the rulemaking, HHS did not even consider the criminal provision at all or the charge of obtaining IIHI under it—there is no discussion of either 42 U.S.C. § 1320d-6 or "obtain."

That said, the Privacy Rule is not unenforceable merely because of HHS's drafting. The civil penalties section—the criminal provision's statutory neighbor—penalizes any person who "violates a provision of this part" without specifying that IIHI be obtained. 42 U.S.C. § 1320d–5. So uses of IIHI violating the Privacy Rule could still generate civil liability if the Privacy Rule is under "this part."

B. Because of how Congress drafted HIPAA, the Privacy Rule can never be enforced by the criminal provision because it falls outside of "this part."

The extensive legislative history discussed above, as recounted by HHS itself, leads to a simple conclusion: the Privacy Rule is not within the "this part" that encompasses 42 U.S.C. § 1320d–6, so a violation of that Rule is not a violation of "this part" and does not support criminal liability.

HIPAA Section 262 created Part C of Title XI of the Social Security Act. The provision authorizing HHS to create the Privacy Rule was not found there, but in Section 264. Section 264 does not amend the Social Security Act. So the Privacy Rule itself and the authorizing statutory section is not even part of the Social Security Act, much less part of Part C of Title XI.[6]

This pill might be harder to swallow were it not acknowledged by both HHS and Congress. In addition to the extensive discussion of Section 264 in the HIPAA rulemaking, HHS built an acknowledgement into the regulatory text. It states that the provisions in its HIPAA rules are "adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the [Social Security] Act[and] section 264 of Public Law 104-191." 45 CFR § 164.102. That reflects the understanding that while some provisions, such

[6] While Section 264 has been included in a note to 42 U.S.C. § 1320d–2, that bears no weight in demonstrating that it is included in Part C. A choice of the codifiers of the U.S. Code is given no weight in its interpretation. *See North Dakota v. United States*, 460 U.S. 300, 311 n.13 (1983).

as the definition of "covered entity" contained in the Privacy Rule, are adopted pursuant to authority in Part C, others (the actual privacy provisions of the Privacy Rule) are *not*. Congress later added an additional section to Part C of Title XI of the Social Security Act. Trauma Care Systems Planning and Development Act of 2007, Pub. Law 110–23, 121 Stat 90 (2007), § 105. It directs HHS to revise the Privacy Rule to limit use of genetic information. 42 U.S.C. § 1320d–9(a). In doing so, it defines the term "HIPAA privacy regulation" to mean "the regulations promulgated by the Secretary under this part *and section 264* of [HIPAA]." *Id.* § 1320d–9(b)(3) (emphasis added). Congress recognizes the difference.

Indeed, in that same provision, Congress acted as if the Privacy Rule might not generate criminal liability. It specified that any covered entity that

> violates the HIPAA privacy regulation (as revised under subsection (a) or otherwise) with respect to the use or disclosure of genetic information shall be subject to the penalties described in sections 1320d–5 and 1320d–6 of this title in the same manner and to the same extent that such penalties apply to violations of this part.

Id. § 1320d–9(d). If the Privacy Rule itself were sufficient to generate liability, that provision would be unnecessary. And if Congress wanted to make any violation of the Privacy Rule generate liability, it could have simply not included the limitation to only genetic information rules.

Instead, when Congress has liked something about the Privacy Rule, it has simply incorporated it into the statute. For instance, in the criminal provision itself,

Congress incorporated the definition of covered entity from the Privacy Rule (though not from Section 264). 42 U.S.C. § 1320d–6(a).

Thus, the Privacy Rule is not included in "this part" and a violation of it cannot support a criminal HIPAA charge.

C. Criminalizing a violation of the Privacy Rule would violate the Constitution in multiple ways.

To begin, allowing an administrative agency to create complex regulations subject to severe felony penalties for violations thereof raises substantial non-delegation concerns. The en banc Fifth Circuit in *Cargill v. Garland* reached its holding of rejecting the ATF regulations at issue on other grounds (including the rule of lenity and that *Chevron* deference did not apply to criminal statutes), but it noted the nondelegation concerns raised by ATF regulations generating criminal liability. 57 F.4th 447, 471 (5th Cir. 2023) (en banc), *aff'd*, 602 U.S. 406 (2024). While the primary concern there was the lack of explicit authorization for ATF to interpret a criminal statute, the Fifth Circuit swept more broadly, also implicating any regulations with criminal effect:

> For many jurists, the question of Congress's delegating legislative power to the Executive in the context of criminal statutes raises serious constitutional concerns. . . . We do not reach this issue because we do not have to. But if we did, it would only provide more support for [our] conclusion . . . .

Id. at 472. *See also id.* at 471 (noting that five current Justices have "call[ed] into question the relevant standards for legislative-power-delegation issues").[7] The en banc Fifth Circuit stated that this serious constitutional question implicates the canon of constitutional avoidance. *Id.* Here, the same issues are at work and the same result should follow. Because turning HHS's Privacy Rule into a criminal regime would raise serious constitutional questions, especially given the lack of clear congressional intention to do so, the obvious alternative path of construing the criminal provision *not* to incorporate the Privacy Rule should be taken.

The rule of lenity counsels the same conclusion. If Congress's intent not to clothe the Privacy Rule with criminal effect is unclear, it is at best "grievously ambiguous" whether Congress intended to do so. *See id.* As *Cargill* notes, the "rule of lenity also prevents the possibility whereby Congress passes an ambiguous criminal statute, only to be interpreted later by a federal agency." *Id.* The Privacy Rule should not be enforced criminally.

These conclusions make sense. Beyond the issues with converting complex administrative regulations into criminal law, the Privacy Rule is simply not drafted with the precision of an ordinary criminal statute.[8] There is no evidence that HHS

[7] While the Fourth Circuit rejected a non-delegation challenge to the Privacy Rule at the time of its promulgation, the challenge focused on the lack of an intelligible principle rather than the criminal nature of the potential effect. *S.C. Med. Ass'n v. Thompson*, 327 F.3d 346, 350–52 (4th Cir. 2003).

[8] For just one example, one of the potential defenses is an ungrammatical mess. *See* Dkt. No. 41 at 11 (discussing 45 C.F.R. § 164.512(j)).

thought it was drafting a criminally enforceable provision, much less that it thought through the consequences of doing so.

* * *

Throughout HIPAA's tortured history, Congress and HHS have failed to firmly fix the most basic of health information privacy violations as crimes. Yet those provisions have largely avoided the close examination that a criminal case invites. Now that the government has overreached in charging a case under those untested provisions, and done so poorly at that, it is clear that HIPAA cannot bear the weight placed on it.

CONCLUSION

The superseding indictment should be dismissed with prejudice. The law simply does not criminalize what the government alleges Dr. Haim did. To the extent that the government seeks to maintain this case, it should explain why the law should bend beyond the breaking point on appeal.

Counsel for Dr. Haim has conferred by email with counsel for the government. The government opposes the relief requested herein.

The defense requests a hearing on this motion.

Dated: October 31, 2024

Respectfully submitted,

Ryan Patrick
Attorney-in-Charge
TX State Bar 24049274
SDTX No. 3006419
Haynes and Boone LLP
1221 McKinney Street, Suite 4000
Houston, Texas 77010
Tel: 713.547.2000
Fax: 713.547.2600
ryan.patrick@haynesboone.com

Mark D. Lytle
DC Bar 1765392
SDTX No. 3884197
Nixon Peabody LLP
799 9th Street NW, Suite 500
Washington, D.C. 20001
Tel: 202.585.8435
Fax: 202.585.8080
mlytle@nixonpeabody.com

/s/ Marcella Burke
Marcella C. Burke
TX State Bar 24080734
SDTX No. 1692341
Burke Law Group, PLLC
1000 Main St., Suite 2300
Houston, TX 77002
Tel: 832.987.2214
Fax: 832.793.0045
marcella@burkegroup.law

/s/ Jeffrey Hall
Jeffrey A. Hall
VA State Bar 82175
SDTX No. 3885025
Burke Law Group, PLLC
2001 L. Street N.W., Suite 500
Washington, D.C. 20036
Tel: 832.968.7564
Fax: 832.793.0045
jeff@burkegroup.law

ATTORNEYS FOR DEFENDANT EITHAN DAVID HAIM

CERTIFICATE OF SERVICE

The undersigned attorney hereby certifies that a true and correct copy of the above and foregoing document has been filed and served on October 31, 2024 using the CM/ECF system, which will send notification of such filing to all counsel of record.

/s/ *Marcella C. Burke*
Marcella C. Burke

CERTIFICATE OF CONFERENCE

I hereby certify that on October 31, 2024, counsel for the defense conferred via email with counsel for the government Tina Ansari who confirmed that the relief requested herein was opposed.

/s/ *Marcella C. Burke*
Marcella C. Burke