**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

**FREDERICK C. TROTTER,**

*Plaintiff,*

**v.**

**CENTER FOR MEDICARE AND MEDICAID SERVICES,**

*Defendant.*

**Case No. 1:19-cv-2008-RCL**

# MEMORANDUM OPINION

Plaintiff Frederick C. Trotter wanted information about millions of doctors, nurses, and other healthcare providers from the Center for Medicare and Medicaid Services (CMS). Specifically, he asked CMS to disclose to him the domain portion of the email address associated with each healthcare provider registered with CMS, along with the provider's national provider identification number.[1] CMS denied his request, claiming that disclosing that information would invade the healthcare providers' privacy. So, Trotter sued under the Freedom of Information Act (FOIA), seeking to compel disclosure.

Both parties seek summary judgment.

Upon consideration of the motions (ECF Nos. 23, 25), briefs (ECF Nos. 23-2, 24-1, 25-1, 28, 29, 30), declarations (ECF Nos. 23-3, 24-2, 25-2, 28-2, 28 -3, 28-4), and all other pertinent papers of record, the Court will **GRANT IN PART** and **DENY IN PART** CMS's motion for summary judgment and **GRANT IN PART** and **DENY IN PART** Trotter's cross-motion for summary judgment.

[1] An email address consists of a local-part, the "@" symbol, and a domain. For example, in the email address bevo@utexas.edu, "bevo" is the local-part and "utexas.edu" is the domain.

## I. BACKGROUND

Federal regulations require virtually every healthcare provider to register with CMS and obtain a unique identification number, known as a "national provider identification" number. *See generally* 45 C.F.R. ch. 162. To obtain a national provider identification number, healthcare providers must register with a database called the "national plan and provider and enumeration system." Schell Decl. ¶ 6 (ECF No. 28-4). When registering, healthcare providers must provide contact information—including an email address—for someone who can answer questions about the provider's application. *Id.* The email address need not be for the provider himself, but each email address must belong to a person, as opposed to an entity or corporation. *Id.*

Trotter submitted a FOIA request for the email address associated with each national provider identification number. Gilmore Decl. ¶ 5. CMS identified 6,380,915 active providers. *Id.* at ¶ 15. After CMS informed Trotter it would withhold the full email addresses to protect the healthcare providers' privacy, *id.* at ¶ 7, Trotter amended his request to ask only for the *domains* associated with each provider, *id.* at ¶ 8. Again, CMS asserted the providers' privacy interests and refused to release the domains. *Id.* at ¶ 12. After exhausting his administrative remedies, *id.* at ¶ 13, Trotter filed this suit.

## II. LEGAL STANDARDS

### A. Freedom of Information Act

FOIA establishes an enforceable right to federal agency records, unless one of the act's exemptions applies. 5 U.S.C. § 552(a), (b). Information is presumptively subject to disclosure. *Dep't of State v. Ray*, 502 U.S. 164, 173 (1991). An agency that withholds responsive documents, bears the burden of proving that one of FOIA's exemptions allows it to decline to disclose the information. *DiBacco v. Dep't of the Army*, 926 F.3d 827, 834 (D.C. Cir. 2019).

Relevant here is the sixth of FOIA's nine exemptions, which shields from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." *Id.* at § 552(b)(6). In determining whether the personal privacy exemption applies, the Court conducts a four-step inquiry. *Aqualliance v. Army Corps of Eng'rs,* 243 F. Supp. 3d 193, 197 (D.D.C. 2017).

First, the Court must determine whether the information at issue is a "personnel and medical file[] [or] similar file[]"—that is, whether the information relates to a particular individual. *See Dep't of State v. Wash. Post Co.*, 456 U.S. 595, 599–603 (1982).

Second, the Court must determine whether the individual has a cognizable privacy interest in the information. In determining whether a privacy interest exists, the Court looks to both the common law and common understandings of privacy. *See Nat'l Archives & Records Admin. v. Favish*, 541 U.S. 157, 167 (2004). Those standards allow for a broad range of privacy interests: both "intimate" and "prosaic" information may be protected. *Painting & Drywall Work Pres. Fund, Inc. v. Dep't of Hous. & Urban Dev.*, 936 F.2d 1300, 1302 (D.C. Cir. 1991). When a privacy interest exists, it belongs to and exists to protect the individual, not the government. *See U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763–65 (1989). Most corporations cannot claim the privacy exemption, *see FCC v. AT&T, Inc.*, 562 U.S. 397, 403 (2011), but closely held corporations and other similar entities can, *Multi Ag Media LLC v. USDA*, 515 F.3d 1224, 1228-29 (D.C. Cir. 2008).

Third, the requester must demonstrate that disclosure of the information serves a significant public interest. *See Roth v. Dep't of Justice*, 642 F.3d 1161, 1174–75 (D.C. Cir. 2011). Releasing information serves a significant public interest when it informs the public about agency actions. *See Citizens for Responsibility & Ethics in Washington v. Dep't of Justice*, 746 F.3d 1082, 1093

(D.C. Cir. 2014). Whatever interest the requester asserts must be held by the public at large; a requester's personal interest in the information is irrelevant. *Reporters Comm.*, 489 U.S. at 771–72.

Fourth, the Court must balance the individual interest in privacy against the public interest in disclosure. If the agency demonstrates that the individual interest in privacy outweighs the public interest in disclosure, it is entitled to exempt the documents from disclosure. *Favish*, 541 U.S. at 172. But if the agency fails to carry its burden, the documents must be disclosed. *See, e.g.*, *Multi Ag*, 515 F.3d at 1233.

The Court reviews an agency's determination not to disclose information *de novo*. 5 U.S.C. § 552(a)(4)(B).

**B. Summary Judgment**

The Court grants summary judgment "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56. The moving party bears the burden of showing its entitlement to summary judgment; the moving party, however, must simply show that the non-moving party has not produced enough evidence to prevail at trial. *See Celotex Corp. v. Catrett*, 477 U.S. 317, 322–23 (1986).

In this posture, the Court construes facts and makes inferences in favor of the non-moving party. *Scott v. Harris*, 550 U.S. 372, 380 (2007). If the parties disagree about material facts, the Court must credit the non-moving party's version. *Robinson v. Pezzat*, 818 F.3d 1, 8 (D.C. Cir. 2016). Facts, however, are disputed only if a reasonable jury could believe either side of the dispute. *See Scott*, 550 U.S. at 380. A fact is material if it is necessary to the Court's decision. *See Johnson v. Perez*, 823 F.3d 701, 705 (D.C. Cir. 2016).

In a FOIA case, an agency is entitled to summary judgment if it can show that (a) it has identified all responsive documents and (b) it has disclosed all responsive documents, except those that fall within an exemption. *DiBacco*, 926 F.3d at 834.

## III. ANALYSIS

Trotter challenges CMS's denial of his request for the domain names of all healthcare providers' email addresses on two grounds. First, he argues that CMS did not conduct an adequate search for records. Second, he argues that the domain information he seeks does not fall under FOIA's privacy exemption. Neither argument passes muster.

### A. Adequacy of Search

Trotter initially argued that CMS has not conducted a search for the records he seeks because it had not provided a search method or search terms in its affidavits. In his reply brief, however, Trotter conceded that argument. Pl.'s Reply 8, ECF No. 30. Now, both parties agree that the information Trotter seeks can be found in a known database. And CMS identified some 6,380,915 relevant fields in that database. No further search could uncover additional relevant documents, so no further search is required. *Morley v. CIA*, 508 F.3d 1108, 1114 (D.C. Cir. 2007).

### B. Privacy Exemption

The Court analyzes whether the privacy exemption applies using the four-part framework set forth above.

#### 1. Applicability of Exemption

First, for the privacy exemption to apply, the information must convey information about a particular individual. *See Wash. Post Co.*, 456 U.S. at 599–603 (1982). Here, the information requested—the email address domain names—does indeed convey information about a particular

individual. That is so because the email address domains all belong to a person.[2] And those domains convey information about the person to which they belong because the domains identify entities with whom the contact persons have a commercial relationship or, in some cases, the providers' own websites. *Cf. Prechtel v. FCC*, 330 F. Supp. 3d 320, 329 (D.D.C. 2018) (email addresses); *Gov't Accountability Project v. Dep't of State*, 699 F. Supp. 2d 97, 106 (D.D.C. 2010) (same). The domains, therefore, qualify protectable information under the privacy exemption.[3]

To argue that that the email address domains do not fall within the FOIA privacy exemption, Trotter offers the following analogy . He argues that disclosing a name is like disclosing only the state portion of a street address. But this analogy is flawed. The privacy exemption would apply to someone's state of residence just as it applies to his email address domain. Though many people share the same state of residence or the same email address domain, both types of information nevertheless convey something particular about an individual. Thus, the Court finds that the email address domain names Trotter seeks satisfy the first requirement for the FOIA privacy exemption requirement.

**2. Individual Privacy Interest**

The second requirement for the FOIA privacy exemption to apply is that the individual has a privacy interest in the information sought. *Favish*, 541 U.S. 157, 167 (2004). Such a privacy

---

[2] Even in cases where the providers are corporations, the contact persons are individuals. Thus, the same analysis applies to both individual providers—doctors, nurses, and the like—and organizational providers—clinics, hospitals, other entities.

[3] To be sure, there are some contexts where email address domains do not convey information about the email address owner. *See, e.g., Bloche v. Dep't of Def.*, 370 F. Supp. 3d 40, 59 (D.D.C. 2019) (rejecting claim of privacy exemption for domains when the agency failed to show how domains could reveal personal information). Take, for example, a FOIA request for the domain of every Department of Justice employee. That each employee's email has a justice.gov domain would not provide any new information about individuals already known to work for the Department. But here, each domain is tied to a national provider identification number. Many of the domains will reveal the providers' employers or companies. Even generic domains, in this context, will reveal at least some personal information about the providers—which email service they use. So here, the providers' domains surmount the low bar to qualify as protectible information.

interest exists when the release of the information requested could reasonably be expected to cause an invasion of personal privacy. *See Favish*, 541 U.S. 157, 167. The government argues that the providers have a privacy interests in their domains because releasing the domains could allow a malicious actor to invade their privacy by targeting them in more effective cyber-attacks. *See* Domizio Decl. at ¶¶ 8–11. It explains that malicious actors use a technique known as spearphishing, which involves using personal information to induce the target to provide other sensitive information. *Id.* The government argues that if a malicious actor could email the providers and include their national provider identification numbers, the providers would be more likely to fall for the spearphishing effort. *Id.* The Court agrees that providers have at least some privacy interest in avoiding spearphishing. *Cf. Long v. Immigration & Customs Enf't*, 464 F. Supp. 3d 409, 419–423 (D.D.C. 2020).

Trotter responds that the providers have surrendered their privacy interest in avoiding spearphishing because CMS already releases some national provider identification numbers paired with domain names. This argument succeeds in part. CMS does provide email addresses in the same location as identification numbers, but only for participants in electronic health information exchange, a digital records-sharing program. *See generally* Dep't Health & Human Servs., *Principles and Strategy for Accelerating Health Information Exchange* (Aug. 7, 2013), https://www.healthit.gov/sites/default/files/acceleratinghieprinciples_strategy.pdf. Providers who participate in heath-information exchange no longer have an interest in maintaining the privacy of their domains because CMS has disclosed this information publicly. But providers who do *not* participate in heath-information exchange still maintain their interest in the privacy of their domains.

Trotter also argues that only solo practitioners could have a privacy interest in their domains, because corporations do not have privacy interests under FOIA. But this argument is a red herring. The privacy interest belongs to the individual. And, as explained above, all of the contacts associated with national provider identification numbers are individuals.

Finally, Trotter argues that disclosure should be required under a CMS regulation. But this is a FOIA action, not an APA suit. The CMS regulation is thus irrelevant. *See Pub. Citizen Health Research Grp. v. Food & Drug Admin.*, 704 F.2d 1280, 1287 (D.C. Cir. 1983).

Therefore, providers who participate in heath-information exchange and who have their email addresses listed within their identification numbers on a CMS website do not have a privacy interest in their domains; all other providers have some privacy interest in their domains.

**3. Public Interest**

Third, as the requester of private information, Trotter must identify a significant public interest and must demonstrate how releasing the information would serve the public interest. *See Roth*, 642 F.3d at 1174–75.

Disclosure serves the public interest by informing the public about agency actions. *See Citizens for Responsibility & Ethics in Washington*, 746 F.3d at 1093. Trotter says that he meets the standard because the "actions of the Defendant are part of, and impact the healthcare system, and the requested data describes that healthcare system." Pl.'s Opp'n 17, ECF No. 24. More specifically, he says that the data will allow the public to "evaluat[e] whether CMS is properly addressing issues of waste, fraud, and abuse."[4] *Id.*; *see also* Trotter Decl. ¶ 40, ECF No. 24-2. In

[4] Trotter also claims that the information will help facilitate epidemiological studies, but he does not explain how those studies would shed light on *CMS's functions* as opposed to public health in general. That claim, therefore, cannot support a significant public interest in releasing the information. *See Roth*, 642 F.3d at 1174–75.

pointing to how an agency addresses waste, fraud, and abuse, Trotter identifies a significant public interest.

Trotter, fails, however, to show a nexus between the information he seeks and how CMS addresses waste, fraud, and abuse. *See Pinson v. Dep't of Justice*, 202 F. Supp. 3d 86, 101 (D.D.C. 2016). Mere speculation does not satisfy this nexus requirement. *Id.* And Trotter offers only speculation that the public could use domains to learn about waste, fraud, and abuse.

His logic on this prong follows an attenuated, three-step path. First, he suggests—without evidence—that linking a provider to a domain may allow the public to determine to which organization a provider is primarily connected. Trotter Decl. ¶¶ 37–38. Second, he suggests that the public could combine information about a provider's primary organization with information about the organization's policies to examine the organization's "clinical approach[]." *Id.* at ¶¶ 39–40. Third, he suggests that the public could use that data to understand how some organizations respond to financial incentives provided by CMS. *Id.* at ¶¶ 39–40. And fourth, he explains that information about responses to CMS financial incentives will lead to information about waste, fraud, and abuse.

Trotter's logic is too tenuous to establish the necessary nexus. *Cf. Consumers' Checkbook Ctr. for the Study of Servs. v. Dep't of Health & Human Servs.*, 554 F.3d 1046, 1054–55 (D.C. Cir. 2009) (declining to release private CMS data given absence of specific allegations of fraud to support asserted public interest in detecting fraud). Trotter's first link is speculative because he provides no reason to believe that a provider's domain has any connection to his primary organization; a provider could just as easily stick with whichever email address he obtained first out of convenience. Trotter's second link is speculative because he does not explain how knowledge about a provider's primary organization leads to information about clinical approach;

he simply assumes that one follows the other. Trotter's third link is the most sound: information about an organization's clinical approach may provide data about how organizations respond to CMS policies. But Trotter's fourth link is the most speculative: rather than alleging that waste, fraud, and abuse is occurring, he speculates that developing information about financial incentives will automatically uncover waste, fraud, and abuse. Trotter provides no specific reasons to believe that the data would be useful in detecting waste, fraud, or abuse. And his generalized concerns, "do[] not raise a cognizable public interest under FOIA in verifying that CMS is adequately detecting fraud." *Id.* at 1054. Therefore, Trotter cannot meet his burden to establish a significant public interest in disclosing the information he seeks.

**4. Balancing**

Finally, the Court must balance the individual interest in privacy against the public interest in disclosure. Here, while the government has demonstrated privacy interests in shielding the domains of providers who do not participate in heath-information exchange, Trotter has identified no public interest in disclosing them. The privacy interest thus outweighs the public interest in disclosure. Therefore, the domains of providers who do not participate in heath-information exchange are exempt from disclosure. *See id.* at 1054.

The domains of providers who participate in heath-information exchange, however, must be disclosed because exempting them from disclosure serves no privacy interests.

## IV. CONCLUSION

Based on the foregoing, the Court will **GRANT IN PART** and **DENY IN PART** CMS's motion for summary judgment, ECF No. 23, and **GRANT IN PART** and **DENY IN PART** Trotter's cross-motion for summary judgment, ECF No. 25. The Court will require CMS to disclose the domains and identification numbers only of providers who (1) participate in health-

information exchange and (2) have their email addresses and provider identification numbers listed together in the National Plan and Provider Enumeration System.

Date: 2/8/21

Royce C. Lamberth
United States District Judge