IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
v.	)	**No. 1:19-cr-10043-STA**
	)	
LORAN KARLOSKY, M.D. *et al.*	)	

MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS PATIENTS' MEDICAL RECORDS UNCONSTITUTIONALLY AND IMPROPERLY SEIZED

I. Factual Background.

A. Downtown Medical Clinic maintained patient records in electronic storage.

Downtown Medical Clinic operated between 2013 and 2016 and was owned by Dr. Karlosky and Dr. Shires; it was staffed by Mary Ann Bond, the nurse practitioner hired to provide direct patient care. The clinic used Practice Fusion, an electronic medical records company, to update and maintain its patient files. *Cf.* 42 U.S.C. § 300jj-11(c)(3)(A)(ii).

B. The government obtained the clinic's electronic medical records by court order.

In 2015, state and federal law enforcement took notice of Ms. Bond's controlled substance prescribing practices. (Shires Motion, Doc. 125, PageID 379).[1] In December 2016, the Tennessee Bureau of Investigation, which continues to be one of the investigating agencies supporting this prosecution,[2] obtained a state court order to receive the clinic's patient records electronically stored with Practice Fusion pursuant to 18 U.S.C. §§ 2703(c)(1)(B), (d). (DOJ_0009521).[3] The state court

[1] During the investigation, the Department of Health obtained certified copies of Clinic records and certifications that certain requested records did not exist. (*Id.*, PageID 381.)

[2] *See* (Government's Expert Notice, Doc. 124-1) (identifying TBI agent as expert witness).

[3] Whereas § 2703(b) governs order for the "contents" of electronic communications, § 2703(c) governs records of electronic communications "not including the contents of communications." 2703(c)(1). These bates numbers refer to the government's discovery production in this case; the discovery materials concerning acquisition of Practice Fusion records cited in this motion are attached as collective **EXHIBIT 1.**

granted the application and ordered Practice Fusion to disclose "the complete and accurate medical records" of 91 patients. (DOJ_0009526–30.) The application and order were sealed. (DOJ_0009534.)

"Practice Fusion responded that it was unable to provide the records in the patient-by-patient format requested, so TBI obtained a second order in early 2017…." (Government's Response, Doc. 138, PageID 579). Practice Fusion also questioned whether the order to seal, which cited 18 U.S.C. § 2703(d), applied to the court order. (DOJ_0009537.)

In January 2017, the TBI re-applied for a state court order to obtain Practice Fusion records, again pursuant 18 U.S.C. §§ 2703(c)(1)(B), (d). (DOJ_0009540). The asserted bases for "reasonable grounds" to obtain the court order were: (1) information from Dr. Karlosky that the clinic's medical records are maintained by Practice Fusion,[4] (2) a statement that investigations "exposed an extraordinary quantity of prescriptions written for controlled substances originating at the Downtown Medical Clinic diverted for illicit non-medical purposes," (3) a statement that evidence seized at a pharmacy "demonstrated a high volume of narcotic prescriptions" written by Ms. Bond, (4) allegations by an unnamed former clinic employee about Ms. Bond's overprescribing, insurance billing, and the use of a separate mobile phone app, Epocrates, "to enter narcotic prescriptions," and (5) citations to laws for record maintenance. (DOJ_0009542). The application further stated that "the specific patient records are narrow in scope," although the resulting court order directed Practice Fusion to disclose "complete and accurate…medical records for the Downtown Medical Clinic," and did not specify particular patients. *See* (DOJ_0009541; DOJ_0009546.) The order to seal was pursuant to 18 U.S.C. § 275(a).[5] (DOJ_0009551.).

[4] The application did not mention Dr. Shires' ownership interest.

[5] Presumably, this was supposed to be § 2705(a). *See* (DOJ_0009549). Section 2705(a) allows for delayed notification when a governmental entity is acting under § 2703(b).

Practice Fusion informed the TBI that it was "waiting on documentation regarding proof of notice sent to the providers," Dr. Karlosky and Ms. Bond. (DOJ_0009555). Thereafter, in March 2017, the TBI served notice on Dr. Karlosky that the "State of Tennessee…has made application for an order" pursuant to 18 U.S.C. §§ 2703(c)(1)(B), (d) "directing Practice Fusion…to disclose records and other information pertaining to…Downtown Medical Clinic…." (DOJ_0009559). The notice did not specify the nature of the law enforcement inquiry or any information concerning the scope of records sought. *Cf.* 18 U.S.C. § 2705(a)(5) (specifying content of related notice).

In April 2017, Practice Fusion delivered the requested materials by sending a link to the government to access the documents. (DOJ_0009577). "The production was voluminous and included numerous spreadsheets, images of scans, and other files." (Government's Response, Doc. 138, PageID 579). Among the materials produced by Practice Fusion were "print-outs of the 97 patient charts associated with the specific patients you identified." (Doc. 138-1, PageID 589). Communication between the government and Practice Fusion has continued over the course of this prosecution, resulting in references to at least one "most recent production." (*Id.*, PageID 580).[6]

C. The government obtained the clinic's medical records during Dr. Shires' arrest, though an early search warrant apparently went un-executed.

In 2019, fifteen boxes of records, including some that "look like…the interface that Practice fusion uses to display patient files" and were "obtained by consent…from Dr. Shires at the time of his arrest." (Transcript, Doc. 179, PageID 957–58).[7] However, based on a document provided in discovery titled "records search warrant" (originally produced in discovery on May 15, 2019, and reproduced on June 14, 2021), it appears government agents previously planned to

[6] Practice Fusion's productions caused "frustration" because they were "produced to the government in a fashion that makes them difficult to navigate, synthesize and, sometimes, understand." (Government's Response, Doc. 138, PageID 578).

[7] Dr. Karlosky is also filing a motion to suppress the records obtained from Dr. Shires.

obtain the medical records from Dr. Shires' house by search warrant. The document, attached as **EXHIBIT 2**, includes a draft affidavit that informs, "Doug Pate [TBI] attempted to obtain the electronic medical records from Practice Fusion….The general counsel said they had never fulfilled such a request for records, but they worked with Pate and provided him with the requested data after months of discussions and a judicial subpoena…." (*Id.*, Page 5). In another Tennessee prosecution for alleged violations of the CSA by medical professionals, the government obtained a search warrant. *See* Warrant, *In the Matter of the Search of information associated with Dr. Henry Babenco/Lafollette Wellness Center that is stored electronically by premises controlled by Practice Fusion*, No. 3:19-MJ-2019 (E.D. Tenn. Feb. 7, 2019), attached as **EXHIBIT 3**.

D. The government re-obtained the clinic's electronic medical records and other information by trial subpoena directed to Practice Fusion.

In 2020, the government re-obtained the clinic's patient medical records using a trial subpoena directed to Practice Fusion. As explained in an earlier filing, "Pursuant to discussions with outside counsel for Practice Fusion about formatting improvement, the government recently issued a trial subpoena commanding Practice Fusion to reproduce all of the Downtown Medical records…." (Doc. 138, PageID 580). *See also* (Tr., Doc. 179, PageID 942) (AUSA Pennebaker: "And we've had them reproduce to use the data in a more mailable format."). The trial subpoena resulted in the disclosure of additional content. (*Id.*, PageID 943) ("Practice Fusion has now given us an explanation of what each of the spread sheets they provided contain.").[8]

The government's experts have been reviewing the medical records from the Practice Fusion production, to include the records for the patients identified in Counts 2 through 8 of the indictment. (Doc. 138, PageID 586). When this Court reviewed the government's expert witness

[8] The defense has not been able to locate a copy of the trial subpoena in discovery, and it does not appear that a return has been filed with the clerk.

disclosures in response to a motion by Dr. Shires to exclude the witness's testimony, the Court noted that the witness's opinions were based on "individualized analysis of patient records from Downtown Medical Clinic." (Doc. 175, PageID 894). The Court also noted the government's explanation that its witness "needed time to review the most recent production of medical records from Downtown Medical Clinic's third-party vendor Practice Fusion." (Doc. 175, PageID 901).

E. The government has investigated and resolved claims against Practice Fusion.

At a hearing before this Court in May, the government stated: "When Downtown Medical chose [Practice Fusion] as its EMR software, it was free to use. It generated revenue through adds that were inside of the software. And they've gotten in a little bit of trouble about that, but that's neither here nor there." (Transcript, Doc. 179, PageID 940). In fact, in January 2020, Practice Fusion agreed to resolve criminal and civil investigations concerning its electronic health records software and allegations including that it "caused its users to submit false claims for federal incentive payments by misrepresenting the capabilities of its EHR software." *See* Dep't of Justice, *Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations* (Jan. 27, 2020) (hereafter "DOJ Practice Fusion Statement").[9] Practice Fusion admitted soliciting and receiving kickbacks from an opioid company and agreed to pay $145 million. Practice Fusion further agreed "to cooperate fully" with the government including wide disclosures of Practice Fusion's information, records, and documents.[10] *Cf.* (Doc. 179, PageID 944) ("[T]he Practice Fusion programmers and lawyers are committed to helping on this issue.").

[9] Available at https://www.justice.gov/usao-vt/pr/electronic-health-records-vendor-pay-largest-criminal-fine-vermont-history-and-total-145. *See also* Dep't of Justice, *Former Practice Fusion Sales Executive Pleads Guilty to Obstructing Government Investigations Into Purdue Pharma And Practice Fusion* (Mar. 8, 2021), https://www.justice.gov/usao-vt/pr/former-practice-fusion-sales-executive-pleads-guilty-obstructing-government.

[10] *See* (Deferred Prosecution Agreement, attached hereto as **EXHIBIT 4**, ¶¶ 6, 7).

II. Legal Standards.

A. The Fourth Amendment protects privacy interests from government intrusion.

The Fourth Amendment provides, in part, that the "right" to be secure in one's "papers[] and effects" is protected against unreasonable searches and seizures insofar as "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. This amendment was intended to "safeguard the privacy and security of individuals against arbitrary invasions of government officials." *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967). "[N]o single rubric definitively resolves" which privacy interests are protected, but "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2213–14 (2018) (internal citations omitted). A warrantless search is "reasonable only if it falls within a specific exception to the warrant requirement." *Id.* at 2221. The government has the burden of proving that a valid exception to the warrant requirement applies. *United States v. Kinney*, 638 F.2d 941, 943 (6th Cir. 1981) (citing *Vale v. Louisiana*, 399 U.S. 30 (1970)).

i. Probable cause is required to obtain a warrant, and it must be particular.

Law enforcement may only obtain information or items protected by a reasonable expectation of privacy via a search warrant based on probable cause. *See Katz v. United States*, 389 U.S. 347, 351–52 (1967); *Boyd v. United States*, 116 U.S. 616, 630 (1886) (holding principles "apply to all invasions on the part of the government…of the sanctity of…the privacies of life"). A warrant must particularly describe the place to be searched because the Framers enacted the Fourth Amendment to protect against "general warrants." *See Marron v. United States*, 275 U.S.

192, 195–96 (1927); *see also Stanford v. Texas*, 379 U.S. 476, 511–12 (1965) (constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain"). The particularity requirement also requires time limitations. *United States v. Lazar*, 604 F.3d 230, 238 (6th Cir. 2010) (ordering suppression of patient filed seized beyond list's scope and non-patient file evidence).

ii. An expectation of privacy exists for commercial premises and medical records.

The Fourth Amendment's protection extends to "commercial premises" because it "has long been settled that one has standing to object to a search of his office, as well as of his home." *Mancusi v. DeForte*, 392 U.S. 364, 367, 369 (1968); *United States v. Newman*, No. 3:19-CR-59-TAV-DCP, 2020 U.S. Dist. LEXIS 221891, at *17 (E.D. Tenn. Sep. 8, 2020) (concluding defendant clinic owner/medical director had cognizable privacy interest, though he did not treat patients and only reviewed files weekly). Additionally, a constitutionally protected privacy interest exists for medical records. *See Griswold v. Connecticut*, 381 U.S. 479, 484–85 (1965) (recognizing fundamental privacy right protected as penumbral constitutional right, recognized in statutory law, and further protected by public policy); *Planned Parenthood v. Casey*, 505 U.S. 833, 883 (1992) (citing constitutional right of privacy between pregnant woman and physician). *Cf. General Motors Corp. v. Director of Nat. Institute of Occupational Safety and Health*, 636 F.2d 163, 166 (6th Cir. 1980) (recognizing constitutionally protected interest in confidentiality of personal medical records). *Accord* Health Insurance Portability and Accountability Act of 1996 (HIPAA), codified at 42 U.S.C. §§ 1320d–1320d-9. *E.g.*, 45 C.F.R. § 164.502(a) (providing covered entity may not disclose protected health information, except as permitted or required); *McNiel v. Cooper*,

241 S.W.3d 886, 894–95 (Tenn. Ct. App. 2007) ("A patient's expectation that his or her medical records will remain private has constitutional, statutory, and decisional protection in Tennessee.").

In *Ferguson v. City of Charleston*, the Supreme Court held that state agents obtaining medical information, absent a warrant and without the consent of the patient, implicated the patient's Fourth Amendment right to privacy in the protected health information and constituted a warrantless search and seizure under the Fourth Amendment. *See* 532 U.S. 67, 76 (2001) (citing *New Jersey v. T.L.O.*, 469 U.S. 325, 335–37 (1985)). "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital [or medical office] is that the results of those tests will not be shared with nonmedical personnel without her consent." *Id.* at 78. An "intrusion on that expectation may have adverse consequences because it may deter patients from receiving needed medical care." *Id.* at 78 n.14 (citing *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977)); *see also State v. Eads,* 154 N.E.3d 538, 548 (Ohio Ct. App. 2020) ("Similar to the cell phone location data at issue in *Carpenter*, the medical records…revealing Eads' use of alcohol, drugs of abuse, and controlled substances are equally deserving of protection because of their 'deeply revealing nature' and 'provi[sion] [of] an intimate window into [Eads'] life.'").[11]

iii. Privacy interests persists even when records are held by third parties.

A reasonable expectation of privacy is not extinguished because materials are held, and can be accessed by, a third party. *See Carpenter*, 138 S. Ct. 2206 (concluding individual maintains legitimate expectation of privacy in records created and kept by wireless carrier); *Riley v.*

[11] The Sixth Circuit has implicitly acknowledged that patients have a reasonable expectation for a degree of confidentiality in their medical information. *See Lee v. City of Columbus*, 636 F.3d 245, 260-61 (6th Cir. 2011); *Moore v. Prevo*, 379 Fed. App'x 425, 428 (6th Cir. 2010). *But cf. Jarvis v. Wellman*, 52 F.3d 125, 126 (6th Cir. 1995) (finding defendants entitled to qualified immunity because disclosure of medical records did not violate constitution) (deciding the issue, however, 6 years before the Supreme Court's holding in *Ferguson v. City of Charleston*, 532 U.S. 67, 76 (2001), *supra*).

California, 573 U.S. 373, 400–02 (2014) (rejecting argument that law enforcement should always be able to search suspect's call logs without warrant).[12] For example, in *United States v. Warshak*, the Sixth Circuit considered whether the Stored Communications Act allowed the warrantless seizure of the defendant's personal and business emails from the third-party ISP. 631 F.3d 266, 283–88 (6th Cir. 2010). The court determined that the defendant "plainly" had a subjective expectation of privacy in the emails, given the amount of detail they contained about his "business and personal life," and stated that "it would defy common sense to afford emails lesser Fourth Amendment protection" than is granted to other similar forms of communication, such as letters or telephone calls. *Id*. at 284, 285–86 (citation omitted). That emails were "stored with, sent or received through, a commercial [internet service provider]" was a "paramount Fourth Amendment consideration" but did not change the conclusion. *Id.* at 285–88 (holding unconstitutional provisions of SCA that allow warrantless seizure of emails stored on a third-party server).

Based on *Warshak*, the DOJ apparently changed its policy to require warrants for content. Report, Email Privacy Act, H.R. Rep. No. 114-528, at 9 (2016) ("The Sixth Circuit is the only circuit court in the country which has held that a warrant is required for all communications content…Soon after the decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.")[13] After *Warshak*, the Supreme Court also expressly pointed to the widespread use of cloud-based services as a factor *increasing* the privacy concerns implicated by cell phone searches. *See Riley*, 573 U.S. 398–99. The Court

[12] *See United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (email); *R.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F. Supp.2d 1128, 1142 (D.C. Minn. 2012) (private social media messages); *State v. Clampitt*, 364 S.W.3d 605, 607-13 (Mo. App. 2012) (declaring SCA unconstitutional to extent allows law enforcement to obtain text message without warrant).

[13] https://www.congress.gov/congressional-report/114th-congress/house-report/528.

has further indicated that the "third-party doctrine" is not absolute, *see Ferguson*, 532 U.S. at 78, and particularly "ill suited to the digital age," *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

B. Instruments other than warrants may be used in limited circumstances.

In some situations, and for limited purposes, the government may seek records by means other than a search warrant. For example, the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*,[14] prohibits the disclosure of the *content* of electronic communications except in specific circumstances. *See* 18 U.S.C. § 2702(b)(2). Section 2703 is one such exception, and its provisions governing disclosure distinguish between the content of electronic communications and mere records of electronic communications, requiring search warrants for some and court orders for others. *Compare* 18 U.S.C. § 2703(b)(1) (requiring search warrant to obtain content of electronic communications without prior notice to the subscriber) *with* § 2703(c)(1) (allowing governmental entities to obtain non-content records by search warrant, court order, or consent).

The term "electronic communication" means, "[A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…." 18 U.S.C. § 2510(12).[15] Non-content records of electronic communication refer to the name, address, telephone connection records (session times and durations), length of service, telephone number or subscriber number, and means of payment. 18 U.S.C. § 2703(c)(2).

[14] The SCA was enacted as Title II of the Electronic Communications Privacy Act, which became law in 1986. *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 829 F.3d 197, 205 (2d Cir. 2016) denied as moot 138 S. Ct. 1186 (2018) (original § 2703 warrant was replaced by CLOUD Act warrant and the issue was moot). "As the government has acknowledged in this litigation, '[t]he SCA was enacted to extend to electronic records privacy protections analogous to those provided by the Fourth Amendment.'" *Id.* at 206.

[15] *See* 18 U.S.C. § 2711(1) (providing terms defined in 18 U.S.C. § 2510 have, respectively, the definitions given such terms in that section).

"Contents" means, in the context of electronic communications, "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

Warrants for information covered by the SCA must comply with the Federal Rules of Criminal Procedure whereas court orders for SCA-covered information must establish "reasonable grounds" to believe the records are "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). Because the showing required to obtain an SCA court order "falls well short of the probable cause required for a warrant," *Carpenter*, 138 S. Ct. at 2221 (citations omitted), the government may only obtain basic identifying information from internet providers, such as their name, address, and connection records. *See United States v. Hart*, No. 3:08-CR-00109-C, 2009 U.S. Dist. LEXIS 72597, at *41–42 (W.D. Ky. July 28, 2009).

C. A party may have standing to vindicate their own and others' rights.

Generally, a party has standing to raise a claim that alleges an injury in fact to his own legal right. *Rakas v. Illinois*, 439 U.S. 128, 139 (1978). In the context of the Fourth Amendment, the court must determine whether the allegedly wrongful search and seizure violated the rights of the party moving to exclude evidence obtained during that search and seizure. *Id.* at 140. A defendant ordinarily only has standing to invoke the exclusionary rule whenever his own constitutional rights have been violated. *See United States v. Payner*, 447 U.S. 727, 732 (1980). However, third parties have standing to contest the constitutional claims of others if three criteria are met:

> The litigant must have suffered an 'injury in fact,' thus giving him or her a 'sufficiently concrete interest' in the outcome of the issue in dispute; the litigant must have a close relation to the third party; and there must exist some hindrance to the third party's ability to protect his or her own interests.

Powers v. Ohio, 499 U.S. 400, 410–11 (1991) (citing *Singleton v. Wulff*, 428 U.S. 106, 112, 113–14, 115–16 (1976)) (internal citations omitted). *See also Griswold*, 381 U.S. at 481; *Barrows v. Jackson*, 346 U.S. 249 (1953)); *Bolton*, 410 U.S. at 188–89.

In the workplace, "[i]t has long been settled that one has standing to object to a search of his office, as well as of his home," even without showing exclusive control. *Mancusi*, 392 U.S. at 369–70. *See also United States v. Mohney*, 949 F.2d 1397, 1403–04 (6th Cir. 1991). Relevant to this determination is whether the defendant took precautions. *See United States v. King*, 227 F.3d 732, 744 (6th Cir. 2001). For example, the fact that an employee had a private office or password protected computer also weighs in favor of a reasonable expectation of privacy in any business documents seized from those locations. *See United States v. Roberts*, No. 3:08-CR-175, 2009 U.S. Dist. LEXIS 123188, at *17-19 (E.D. Tenn. Dec. 21, 2009) (recognizing privacy in materials seized from defendant's office and password-protected laptop).

III. Argument.

The SCA is unconstitutional when interpreted to allow the government to obtain the content of electronic medical records without a warrant. Since the Sixth Circuit reached a similar conclusion with respect to the email in 2010, *see Warshak*, 631 F.3d 266, it has been the DOJ's policy to use warrants, which perhaps explains why the defense has not identified other cases in which the government obtained electronic medical records *without* warrants. Moreover, opinions assuming a warrant is required to obtain electronic medical records are consistent with the Supreme Court's rejection of the government's use of a § 2703(d) court order rather than warrant to obtain records deserving privacy protections. *See Carpenter*, 138 S. Ct. at 2212.

A. The government's reliance on a court order and trial subpoena to obtain clinic patients' medical records violates the Fourth Amendment.

The government violated the Fourth Amendment when it seized records from Practice Fusion without a warrant. Medical records are fundamentally private, Downtown Medical Clinic took steps to maintain their privacy, and the wholesale acquisition of a medical practice's patient records by court order or subpoena is inconsistent with the constitutional limits on government

overreach and requirements for particularized searches when breaching recognized privacy interests. Nor does the fact that newer technology is involved in this case—*i.e.*, electronic medical records stored off-site in a "cloud" server—shift the analysis. *Cf. United States v. Pompy*, No. 18-cr-20454, 2021 U.S. Dist. LEXIS 48995 (E.D. Mich. Mar. 16, 2021) (discussing warrant to search electronic medical records; holding warrant for doctor's office for "all patient records" appliable to patient files stored in EMR "cloud"); *United States v. Newman*, No. 3:19-CR-59-TAV-DCP, 2020 U.S. Dist. LEXIS 221891 (E.D. Tenn. Sep. 8, 2020) (assuming Fourth Amendment applies to EMRs, holding medical director had standing to suppress patient records obtained from EMR system); *United States v. Nasher-Alneam*, 399 F. Supp. 3d 579 (S.D. W. Va. 2019) (granting motion to suppress certain electronic evidence, including medical records); *United States v. Laynes*, 481 F. Supp. 3d 657 (S.D. Oh. 2020) (granting motion to suppress where officers did not have warrant to search phone or cloud storage).

In *Carpenter*, the Supreme Court held that the Stored Communications Act is unconstitutional because it does not require a warrant to obtain cell phone records showing the phone user's location and confirmed that it "never" allowed subpoenas to third parties for a defendant's private records. *Carpenter v. United States*, 138 S. Ct. 2206, 2201 (2018). In *Carpenter*, the government "applied for court orders under the [SCA] to obtain cell phone records" pursuant to the section of the statute that permits compelled disclosure when the government "'offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation.'" The court orders directed the cell phone companies to disclose "records revealing the location of Carpenter's cell phone whenever it made or received calls" over a period of months. *Id.* at 2214. The Court found that such records provide "an intimate window" into an individual's "familial, professional,

religious, and sexual associations." *Id.* at 2217. Although an individual using a cell phone continuously reveals his location to a third-party (*i.e.*, the wireless carrier), the Court held that an individual maintains a legitimate expectation of privacy in the record of his movements. *Id.* at 2217. Despite the privacy interest, the SCA purported to allow the government to seize records under a standard described as a "gigantic" departure from the probable cause standard. *Id.* at 2221. "Consequently," the Court concluded, "Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant." *Id.* at 2221.

With SCA court orders deemed constitutionally deficient, the Court reviewed whether a subpoena might entitle the government to the same information. *Id.* at 2221. The Court quickly disposed of the question. "[T]his Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." *Id.* at 2221. "If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement." *Id.* at 2222.

The Court noted that its decision was a "narrow one," referencing Justice Frankfurter's caution that, "when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'" *Id.* at 2220 (citation omitted). However, the facts and logic of *Carpenter* mirror those before this Court. As in *Carpenter*, the government used a court order under § 2703(d). Unlike *Carpenter* where the content of the data reflected the location of the cell phone when in use over a few months, the content of the data acquired from Practice Fusion included patient medical charts.

In earlier cases, the Court described the kinds of private data on cell phones as including Internet searches revealing symptoms of disease or apps for drug addictions. *Riley*, 573 U.S. at 396; *United States v. Jones*, 565 U. S. 400, 415 (2012) (Sotomayor, J., concurring)

("GPS…reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."); *Warshak*, 631 F.3d at 284 ("[E]mail is frequently used to remind patients and clients of imminent appointments."). Here, the Practice Fusion content did not just *imply* health issues but *revealed* intimate information. Further, unlike *Carpenter*, where the data were compelled from a wireless carrier, which is a clearly covered entity under the SCA, the government used the SCA to compel data from a medical records service.

Although the government had access to some of the clinic's prescribing data based on regulatory oversight regimes, that did not negate the duty to obtain a warrant for materials outside that structure. For example, in *United States v. Motley*, a court denied the defendant's motion to suppress records seized from the state prescription monitoring database with only a subpoena because the defendant did not have an objectively reasonable expectation of privacy in records of controlled substance prescriptions stored in a government database. 443 F. Supp. 3d 1203, 1210–13 (D. Nev. 2020). "An individual's general medical records," the court reasoned, "are substantially different from an individual's prescription drug records." *Id.* at 2013–14. *Accord United States v. Gayden,* 977 F.3d 1146, 1152 (11th Cir. 2020).

Nor can the government's § 2703(d) application effectively serve as a warrant because the government only had to demonstrate "specific and articulable" facts showing "reasonable grounds" to believe that records were "relevant and material" to the criminal investigation. This standard is much lower than the probable cause required for a warrant. *See Carpenter*, 138 S. Ct. at 2221; *Warshak,* 631 F.3d at 288. The government's § 2703(d) application would not meet that higher standard. First, it was inappropriate to rely on information gleaned during state

administrative investigations.[16] Second, a reviewing court would not have allowed the state to so heavily on an unnamed source whose reliability was not established.[17] *See United States v. Coffman*, No. 1:20-CR-10048-STA (W.D. Tenn. July 16, 2021) (granting motion to suppress based on "bare bones" affidavit that included "attenuated and conclusory" assertions). Third, the court order resulted in the seizure of the entirety of the clinic's patient records and files.

The records seized by the government reveal comprehensive information identifying patients, their diagnoses, and actions taken in relation to their medical charts. According to the government, it is precisely the detailed nature of the defendants and their patients that makes the content of the Practice Fusion records valuable. (Doc. 179, PageID 959) ("tells a story about who knew what when"). *Accord* (*id.*, PageID 961). For example, according to the government, "If you know the GUID [identifying patient and provider number] from that spreadsheet…It tells you on this day Dr. Shires logged in. And he, you know, entered in a diagnosis of A, B and C for patient. And then conveniently, thankfully -- I mean, it's a rare bone that they throw us in Practice Fusion, but I think they use the patient's name in the audit log." (*Id.*, PageID 962). Without limits, the court order was effectively an unconstitutional general warrant.

Regarding standing, Dr. Karlosky's third-party interest in the privacy of the patient medical records and personal interests in protecting the clinic's records are implicated by the seizure of the

[16] The TBI's application for a court order to produce the Practice Fusion records relied, in part, on information relayed by Dr. Karlosky to the Tennessee DOH. (DOJ_0009541.) In effect, by relying on a DOH investigator to support its application for a SCA court order, the TBI used the heavily regulated scheme governing the practice of medicine and nursing in Tennessee to gather evidence for its criminal case, impermissibly expanding its criminal discovery authority. *E.g.*, *United States v. Will*, 671 F.2d 963, 967 (6th Cir. 1981).

[17] When probable cause is gained from a confidential source, the issuing judge must have a basis for finding that the source is reliable or credible. *E.g.*, *United States v. Dyer*, 580 F.3d 386, 390 (6th Cir. 2009). When an affidavit contains no information on the informant's reliability, independent police corroboration must be substantial. *United States v. Neal*, 577 F. App'x 434, 440 (6th Cir. 2014), *cert. denied*, 574 U.S. 1094 (2015).

electronic medical records from Practice Fusion. Dr. Karlosky's role as an owner and supervising physician support his standing to contest the government's unconstitutional search and seizure. The records were kept private: clinic employees who used Practice Fusion had a login ID and password to access the records. (DOJ_0001965.) Non-parties to this proceeding were not given notice of their records being shared with the government and have no opportunity to raise the privacy issue themselves. *See Powers*, 499 U.S. at 410–11; *Mancusi*, 392 U.S. at 369–70. The reasonable expectation of privacy in the Practice Fusion records that was not diminished by the records being stored with a third party electronic medical records company. Unlike a state prescription monitoring database, Practice Fusion was a private company. Therefore, the government's interpretation of the SCA to excuse a Fourth Amendment warrant when the *content* of confidential medical records were sought cannot stand. If a category of information more private than one's movements is protected, it must surely be private health records.

A. The SCA court order and trial subpoena were improper.

The government's wholesale seizure of Practice Fusion records cannot stand, even if this Court concludes a warrant was not required, because the government did not sufficiently provide advance notice required by the SCA, and Practice Fusion is not the type of entity governed by the SCA. Similarly, the trial subpoena complies neither with the Fourth Amendment nor with the SCA.

i. The court order did not entitle the government to Practice Fusion content, and any notice was insufficient to establish de facto compliance.

To authorize the production of content rather than mere records about the identifying subscriber information, the SCA requires a governmental entity to proceed under § 2703(b) by providing prior notice to the subscriber. Here, the government proceeded under § 2703(c). While Practice Fusion's actions did, in effect, give prior notice to Dr. Karlosky by delaying disclosure until after Practice Fusion received proof of state's "notice," Practice Fusions actions cannot save

the order. Even if this *de facto* compliance with § 2703(b) were relevant, the notice provided to Dr. Karlosky did not put him on sufficient notice. It did not state with reasonable specificity the nature of the law enforcement inquiry (as required for delayed notification, per § 2705(a)(5)(A)), did not define the scope of the materials sought (as required under Fed. R. Crim. P. 17), did not identify a means of objecting to or quashing the order, did not include telephone or email contact information for anyone involved (*i.e.*, the court clerk or Practice Fusion), and neither identified the person giving notice as a TBI agent nor provided his contact information.[18]

ii. Practice Fusion is not a computing service covered by the SCA.

Whether the electronic medical records at issue are covered by the SCA depends, in part, on whether Practice Fusion is an "electronic communication service" or "remote computing service." 18 U.S.C. § 2510(15), 2711(2). This Court has previously recognized that not all online services are SCA-covered services. *See Inventory Locator Serv., LLC v. Partsbase, Inc.*, No. 02-2695 Ma/V, 2005 U.S. Dist. LEXIS 32680, at *75 (W.D. Tenn. Sep. 2, 2005) (finding that where party operated online marketplace for individuals to buy and sell airplane parts and communicate, it constituted "electronic communication service"). [19]

[18] Provisions for motions to quash or modify were added to § 2703 as subsection (h) in 2018. *See* P..L. 115-278, § 2(g)(2)(I), 132 Stat. 4178.

[19] Decisions from other courts confirm the inevitable conclusion that Practice Fusion is not such a service. *See Garcia v. City of Laredo*, 702 F.3d 788, 792 (5th Cir. 2012) (concluding SCA applies to "providers of a communication service such as telephone companies, Internet or e-mail service providers, and bulletin board services" but *not* to facilities that merely *enable* the "use of electronic services" and provide individual storage); *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1270–72 (N.D. Cal. 2001) (online merchant is not electronic communication service provider); *St. Johns Vein Ctr. v. StreamlineMD Ltd. Liab. Co.,* 347 F. Supp. 3d 1047, 1065 (M.D. Fla. 2018) ("Nothing in the allegations of [the civil Complaint] suggests that the [electronic medical] information management system falls within the definition of an electronic communication system."); *Priority Payment Sys., LLC v. Intrend Software Sols.*, No. 1:15-cv-04140-AT, 2016 U.S. Dist. LEXIS 187881, at *15-16 (N.D. Ga. Nov. 28, 2016) ("[p]rovid[ing] telephone, internet, and email services to its employees in order to perform their job duties does

In *St. Johns Vein Ctr.*, a medical provider claimed that employees of the defendant medical information database company had impermissibly accessed its private patient records under the SCA. 347 F. Supp. 3d at 1055. The medical database software, StreamlineMD, "provide[d] physicians with a license to use its cloud-based integrated software platform to upload a physician's financial and performance data, which the physician can then use to generate reports and other documents on practice management, revenue cycle management, and billing in order to enhance his or her practice." *Id.* at 1053–54. In dismissing the plaintiff's claim regarding the online medical database, the court reasoned that information stored on a cloud-based medical record system was not akin to "e-mails, telephone calls, and communications exchanged on internet websites, electronic bulletin boards, and dropbox systems" housed by "internet service providers, electronic mail providers, telecommunications companies, and remote computing services" and found that nothing about its "information management system falls within the definition of an electronic communication system." *Id.* at 1064 (citing *IPC Sys. v. Garrigan*, No. 1:11-CV-3910-AT, 2012 U.S. Dist. LEXIS 195619, at *9 (N.D. Ga. May 21, 2012)). As an internet-based EMR, Practice Fusion is very similar to the StreamlineMD database at issue in the *St. Johns Vein Ctr.* case. 47 F. Supp. 3d at 1053-54. Because the government relied on the SCA to gain access to Dr. Karlosky's patient files, but the medical records stored on Practice Fusion are not "electronic communications" under the SCA, this process was an improper means to obtain the records.

iii. A trial subpoena cannot obviate pretrial unconstitutional conduct.

---

not make Priority an electronic communication service provider as defined by the SCA") (collecting cases defining "electronic communication service" and limiting that definition to traditional services "such as internet service providers, electronic mail providers, telecommunication companies, and remote computing services."); *In re Nw. Airlines Privacy Litig.*, No. 04-126 (PAM/JSM), 2004 U.S. Dist. LEXIS 10580, at *6 (D. Minn. June 6, 2004) ("Defining electronic communications service to include online merchants or service providers like Northwest [an airline company] stretches the ECPA [SCA] too far.").

At this point, it is not clear what the trial subpoena served on Practice Fusion stated, though it seems reasonable to conclude that, contrary to the plain terms of the standard subpoena to testify at a hearing or trial in a criminal case, *see* AO 89 (Rev. 08/09), Practice Fusion was not directed to bring materials to court but, instead, produced them to the prosecution. In any event, a trial subpoena cannot be used to circumvent the Fourth Amendment for the same reasons a court order premised upon less than probable cause without particularization is unconstitutional.

B. Evidence obtained via these unconstitutional searches should be excluded.

The materials obtained via the initial state court order and subsequent trial subpoena should be excluded from Dr. Karlosky's trial because they were obtained in violation of the Constitution. *See United States v. Laughton*, 409 F.3d 744, 748 (6th Cir. 2005) (reversing denial of motion to suppress). The state court order was objectively unreasonable because Dr. Karlosky and his patients had a reasonable expectation of privacy in the medical records, and such records are not covered by the SCA framework that was used to obtain them. A search warrant is necessary to obtain an individual's personal and business emails held on a third-party server. Therefore, because of the initial order's deficiencies, the derivative tangible and testimonial evidence obtained as a result of the unconstitutional state search warrant must be excluded as "fruit of the poisonous tree." *Wong Sun v. United States*, 371 U.S. 471, 487 (1963); *Murray v. United States*, 487 U.S. 533, 536–37, (1988); *United States v. Sanchez*, No. 20-5136, 2021 U.S. App. LEXIS 3235, at *13-14 (6th Cir. Feb. 4, 2021) (affirming this Court's decision to suppressing a federal warrant as fruit of the poisonous tree because of deficiencies with earlier state warrants).

C. Conclusion.

For the foregoing reasons, Dr. Karlosky moves for suppression of the Practice Fusion records and an evidentiary hearing on this motion.

Respectfully submitted this 17th day of August 2021, by:

RITCHIE, DAVIES, JOHNSON & STOVALL, P.C.

/s/Stephen Ross Johnson
STEPHEN ROSS JOHNSON [BPR No. 022140]
606 W. Main Street, Suite 300
Knoxville, TN 37902
(865) 637-0661
www.rdjs.law
johnson@rdjs.law

THE LAW OFFICE OF MASSEY, MCCLUSKY, MCCLUSKY & FUCHS

/s/William D. Massey
WILLIAM D. MASSEY [BPR No. 9568]
3074 East Road
Memphis, TN 38128
(901) 384-4004
www.masseymcclusky.com
w.massey3074@gmail.com

Counsel for Loran Karlosky, M.D.

CERTIFICATE OF SERVICE

I certify that on August 17th, 2021, a copy of the foregoing was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. All other parties will be served by regular U.S. mail. Parties may access this filing through the Court's electronic filing system.

/s/Stephen Ross Johnson
STEPHEN ROSS JOHNSON