UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY
OWENSBORO DIVISION
CIVIL ACTION NO. 4:17-CV-00017-JHM

CYNTHIA GAY BORUM, as Administratrix of the Estate of Nichole Alyce Borum **PLAINTIFF**

VS.

JUNG WOOK KANG SMITH, MD; DEACONESS CLINIC, INC.; DEACONESS HOSPITAL, INC. and DEACONESS HEALTH SYSTEM, INC. **DEFENDANTS**

MEMORANDUM OPINION AND ORDER

Before the Court is the motion of Defendants (collectively "Deaconess") for a protective order regarding Plaintiff's request to inspect Deaconess' electronic medical records, to have Deaconess provide her with an exact copy of those records in native-format and to allow access to Deaconess' electronic records system during the course of depositions (DN 19). The Plaintiff has responded at DN 21 and Deaconess has replied at DN 26.

Nature of the Case

Plaintiff is the Administratrix of the estate of Nicole Borum. Plaintiff contends that Borum attempted to harm herself in the aftermath of the end of a relationship. Following initial treatment at another hospital, she came under the medical care of Defendant Dr. Smith, who was employed by a Deaconess entity. The Plaintiff alleges that on Borum's second visit, Dr. Smith prescribed an antidepressant. On the third visit Dr. Smith doubled the prescription for a six-month supply and scheduled Borum's next visit a year in the future. Three weeks later Borum

committed suicide. She was twenty-three. Plaintiff claims that the Defendants were negligent in failing to closely monitor Borum's condition notwithstanding a product warning that the medication could increase the risk of suicide in young adults and therefore close supervision was required.

Plaintiff's Discovery Requests

Deaconess employs an electronic medical records ("EMR") system to maintain patient care records, utilizing a software system licensed by Epic Systems Corporation (DN 19). Plaintiff has described her discovery requests to Deaconess:

1. To inspect Borum's medical records in electronic format on Deaconess' computer system;
2. To inspect Deaconess' EMR system's functionality by creating a "test" patient in the system and exploring the system options;
3. To obtain an electronic exact copy of Borum's health information, including all the meta-data and audit trail information concerning her records, and print outs or screen shots of any information Deaconess cannot produce electronically, and;
4. To utilize Deaconess' EMR system during the depositions of medical care providers and corporate representatives "which is the only way Plaintiff can explore the physician's uses and understanding of the system"

(DN 21 at PageID # 327).

Standard of Review

Deaconess seeks protection under Fed. R. Civ. P. 26(c)(1). The rule provides that, upon a showing of good cause, a Court may issue an order "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Id. The party seeking the protective order must establish that good cause exists for the entry of the order by making a "particularized and specific demonstration of fact, as distinguished from stereotyped and conclusory statements." Gulf Oil Co. v. Bernard, 452 U.S. 89, 102 n. 16 (1981). The Court may place limitations on discovery if the information requested is unreasonably cumulative or duplicative or is obtainable from another, more convenient, less burdensome, or less expensive source. Fed

R. Civ. P. 26(b)(2)(C)(i). The Court may also place limitations on discovery if the party seeking discovery has already had ample opportunity to obtain the information sought or the request exceeds the permitted scope of discovery under Rule 26(b)(1). Fed R. Civ. P. 26(b)(2)(C)(i) and (ii).

Rule 26(b)(1), in turn, instructs that the permissible scope of discovery encompasses "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake, the amount in controversy, the parties' relative access to relevant information, the parties' resources and the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Id. Consequently, the two prongs of the discovery analysis are whether the information sought is relevant and whether it is proportional.

1. Plaintiff's Request to Inspect Borum's Records on Deaconess' EMR System

Plaintiff has requested an opportunity to conduct a direct inspection of Borum's medical records in electronic format on Deaconess' computer system. Deaconess advances several arguments in opposition to Plaintiff's request. The first point of opposition is that the requested inspection would require Plaintiff's attorneys or designated representatives to utilize Epic System's software to access the EMR. This, Deaconess argues, would be a violation of the software licensing agreement between Deaconess and designer Epic Systems. Moreover, Deaconess contends that permitting Plaintiff to utilize the software would be an unauthorized use of Epic's programming under the Computer Fraud and Abuse Act ("CFAA") and the Copyright Act of 1976 ("Copyright Act"). Deaconess also argues that Plaintiff's requests implicate restrictions under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d *et seq* (HIPAA).

As a practical matter, Deaconess further contends that the Epic software has been updated several times since Borum received treatment and Deaconess now cannot present the EMR in the exact same manner. Finally, Deaconess argues that, because it has already provided the Plaintiff with a complete copy of Borum's medical records, and Plaintiff has not raised any issues with the completeness or accuracy of those records, there is no relevance to allowing Plaintiff to inspect those same records on Deaconess' EMR system.

A. Violation of the Software Licensing Agreement

Deaconess points out language in the software licensing agreement with Epic Systems which requires Deaconess to "limit access to the Program Property to those of Your employees or other Affiliate users who must have access to the Program Property [to carry out] Your Operations" (DN 19-1, p. 2, referencing DN 19-3, License and Support Agreement at § 11(c)(ii)). Deaconess notes that "affiliate users" are specifically limited in the agreement to individuals and entities involved in its business operations (DN 19-1, p. 2 fn. 1). As such, Deaconess contends that the licensing agreement prohibits any use of Epic System's software for any reason other than patient care and billing purposes, and to permit Plaintiff to utilize the system to explore Borum's EMR would violate that agreement and expose Deaconess to a claim by Epic Systems that it had breached the terms of the contract.

In support of its argument, Deaconess cites Compliance Source, Inc. v. GreenPoint Mortg. Funding, Inc., 624 F.3d 252, 254 (5th Cir. 2010). Deaconess contends that court ruled a party breached its software licensing agreement by allowing its own attorneys to use the software for the licensee's benefit, where the agreement stated the licensee could not "copy, make, use, have made, sell, support, or sub-license" the technology as defined by the contract. Id. at 255.

The Plaintiff responds that federal courts "have broad authority to issue orders governing litigation and discovery, and are not limited by the terms and conditions of private contracts" (DN 21, p. 23). She cites Kebede v. SunTrust Mort. Inc., 612 F. App'x 839, 840 (6th Cir. 2015) for the basic principle that district courts have broad discretion in regulating discovery. While this case does indeed stand for the basic proposition that courts have broad authority, the case says nothing about the impact private contracts may have on discovery.

The undersigned concurs with Plaintiff that Compliance Source, 624 F.3d at 254 does not support Deaconess' position that allowing Plaintiff to access the EMR would cause Deaconess to breach the licensing agreement. In that case, Compliance Source created and licensed mortgage-financing form preparation software for residential lenders, including GreenPoint Mortgage Funding. Id. GreenPoint purchased the software and, notwithstanding a restriction in the licensing agreement that it not allow anyone other than a specifically identified law firm to use the software, allowed outside attorneys not associated with the designated firm to access the software so that they could prepare loans for GreenPoint. Id. at 256. The court concluded that the terms of the licensing agreement did not permit GreenPoint to allow outside parties to use the software, even when that use was for the licensee's benefit. Id. at 260. The case says nothing, however, about whether a licensing agreement constrains the authority of a court to order a party to allow access to the software by an outside party when that access is related to discovery between those parties.

Similarly, another case cited by Deaconess, Centillion Data Sys. v. Ameritech Corp., 193 F.R.D. 550, 553 (S.D. Ind. 1999), does not provide guidance. In that case the defendant sought to discover a settlement agreement between the plaintiff and another entity in a separate matter. The court denied the request on the primary ground that it found the settlement agreement bore

no relevance to the subject action. Additionally, the court noted the effectiveness of contracts providing confidentiality "is an interest the courts will protect." Id. However, this statement must be viewed in the context of the particular case. The court noted that, where an agreement provides for confidentiality, "courts require a strong countervailing interest to breach that confidentiality." Id. That court went on to explain that, while discovery of the agreement might facilitate settlement in that instant case, "settlements are and will be encouraged, in the run of cases, more by maintaining the confidentiality of agreements than by disclosure." Id. The court concluded that the defendant lacked a sufficient interest in the settlement agreement to constitute a sufficiently countervailing interest. Thus, while that court recognized a public policy interest in protecting confidentiality agreements, this was not a blanket rule. The court recognized that the interest in confidentiality must, as in any discovery request, be weighed against relevance and the sufficiency of the requesting party's interest in the information.

Further, it is clear that drawing an analogy between allowing a confidentiality agreement to preclude discovery and allowing a contract to preclude discovery does not support Deaconess' position. Confidentiality clauses do not override a court's ability to order discovery. "Confidentiality clauses in private settlement agreements cannot preclude a court-ordered discovery pursuant to a valid discovery request." Newby v. Enron Corp., 623 F. Supp. 2d 798, 838 (S.D. Tex. 2009) (collecting cases). "A general concern for protecting confidentiality does not equate to privilege . . . . [L]itigants may not shield otherwise discoverable information from disclosure . . . merely by agreeing to maintain its confidentiality." Tanner v. Johnston, No. 2:11-cv-00028-TS-DBP, 2013 U.S. Dist. LEXIS 3512, *4-5 (D. Ut. Jan. 8, 2013) (*quoting* Pia v. Supernova Media, Inc., No. 2:09-cv-840-CW, 2011 U.S. Dist. LEXIS 140396, *1 (D. Ut. 2011)); *see also* United States v. Robinson, No. SA-06-MC-781-XR, 2007 U.S. Dist. LEXIS 14853, *

(W.D. Tex. March 1, 2007) (Private confidentiality agreement will not eclipse a court order of production unless established legal privilege applies.); In re: CFS-Related Secs. Fraud Litig., No. 99-CV-825(K)J Consolidated, 2003 U.S. Dist. LEXIS 15230, *17-18 (N.D. Okla. July 31, 2003) (Confidential settlement agreement discoverable when relevant to claims and defenses in lawsuit.).

A review of the licensing agreement (DN 19-3) makes clear that Epic Systems seeks to protect its software product in two ways. First, it seeks to ensure that the licensee will not utilize the product beyond the agreed scope for which it has paid the licensing fee, thereby protecting Epic System's commercial interest in the contract. Second, it seeks to protect its proprietary software information from public disclosure by allowing access only by the licensee, thereby protecting its commercial interest in the product. As to the first objective, allowing Plaintiff to view the EMR on the system as part of the discovery process does not jeopardize Epic System's commercial interest in the contract, as the use will be for litigation purposes and not delivery of healthcare services. Moreover, Deaconess has not offered any authority clearly supporting the proposition that, by virtue of contracting with a non-party, one party to the litigation can circumvent the rules of procedure and deprive the other litigation party of discovery to which it is otherwise entitled.[1] Additionally, if violation of the licensing agreement were of such concern to Deaconess, they would presumably have notified Epic to allow the software company the opportunity to intervene for the limited purpose of this discovery dispute.

[1] Deaconess has cited Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc., No. 98-1084, 1999 U.S. Dist. LEXIS 6348 (W.D. Penn. May 3, 1999) for the proposition that the court refused to "issue discovery order that places defendant in breach of its licensing agreement, the Copyright Act, or both" (DN 19-1, p. 7). The court made this passing reference in regard to a discovery request for production of third-party software and not in the context of access to a licensee's system. Moreover that court also found that the requested discovery was not relevant to the central inquiry in that case. The lack of analysis in the opinion renders it without precedential value in the current context.

As to Epic System's confidentiality interest, where a party is obligated to protect confidential information which is otherwise discoverable the Court can accommodate the privacy interest while at the same time allowing the other party the discovery to which it is entitled under the civil rules by means of a protective order. First Horizon Nat'l Corp. v. Houston Cas. Co., No. 2:15-cv-2235-SHL-dkv, 2016 U.S. Dist. LEXIS 142332, *37-37 (W.D. Tenn. Oct. 5, 2016). The undersigned therefore concludes that Deaconess' licensing agreement with Epic will not protect it from producing otherwise discoverable information.

B. Statutory Restrictions on Allowing System Access

In addition to breaching the contract with Epic Systems, Deaconess contends that allowing the Plaintiff to access the EMR system would constitute a violation of the Computer Fraud and Abuse Act ("CFAA") and the Copyright Act of 1976 ("Copyright Act"). Deaconess also argues that Plaintiff's requests implicate HIPAA restrictions. None of Deaconess' arguments are availing.

First, Deaconess employs the CFAA (18 U.S.C. § 1032(a)(2)(C)) to support the idea that both Deaconess and the Plaintiff may be civilly and criminally liable should the Plaintiff gain access to the computer system. The cited provision provides that whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer may, under certain circumstances, face criminal liability. 18 U.S.C. §§ 1030(a)(2)(C), 1030(c).

The undersigned cannot locate any published or unpublished opinions from any federal (or state) court supporting a theory that accessing a computer as part of civil discovery violates the CFAA. This is because a court order grants authorized access to the relevant information, and unless the Plaintiff intentionally exceeded the access authorized, there could be no plausible

claim under the CFAA. "The CFAA protects people from unauthorized access to computers, for example by hacking or stealing a password." Brooks Group and Assocs., Inc. v. Levigne, No. 12-2922, 2014 WL 1490529, at 8 (E.D. Pa., Apr. 15, 2014). Nothing suggests it is intended to act as a roadblock to routine discovery requests.[2] *See also* Land and Bay Gauging, LLC v. Shor, 623 Fed. Appx. 674, 683 (5th Cir. 2015) (Debtor could not state a claim under the CFAA because, at time creditor accessed debtor's computers, creditor was doing so pursuant to a court order, and the access was therefore authorized).

Similar reasoning applies to the Defendant's concerns that allowing Plaintiff access to its computer system may violate the Copyright Act. In short, such concerns are simply untenable in the discovery process, assuming the discovering party does not exceed the authority granted by the Court. Analogous arguments have been offered and rejected on numerous occasions. The following list is far from complete but demonstrates courts' apparent unanimity on this issue. *See e.g.* Religious Tech. Ctr.; Church of Scientology Int'l v. Wollersheim, 971 F.2d 364 (9th Cir. 1992) (providing copies of plaintiffs' copyrighted documents to defendants' expert witness constituted fair use); Porter v. United States, 473 F.2d 1329 (5th Cir. 1973) (rejecting a claim by widow of Lee Harvey Oswald that publication of Oswald's writing in the Warren Commission Report diminished their value); Jartech, Inc. v. Clancy, 666 F.2d 403 (9th Cir. 1982) (holding that surreptitiously filming a pornographic film for use in a public nuisance abatement action did not violate the Copyright Act); Carpenter v. Superior Court, 141 Cal. App. 4th 249 (Cal. Ct. App. 2006) (holding that a plaintiff injured in a motorcycle accident could obtain access to certain standardized neurological tests despite objections that providing copies would violate the Copyright Act); Grundberg v. Upjohn, Co., 137 F.R.D. 372 (D. Utah 1991) (district court

[2] The case cited by Deaconess is not relevant to their position. Four Seasons Hotels And Resorts, B.V. v. Consorcio Barr, S.A., 533 F.3d 1349 (11th Cir. 2008) is a decision upholding a district court's confirmation of an arbitral award and primarily concerns considerations of international law.

rejected defendant's attempt to copyright certain discoverable documents to prevent plaintiff's access). In other words, litigants have attempted for years to invoke copyright protection to either capitalize on or avoid the use of certain materials in judicial proceedings and have been consistently unsuccessful. While none of these cases specifically addresses an EMR system, the analogies are instructive, and the undersigned concludes there are no copyright concerns present in this case.

Deaconess next argues that granting Plaintiff's requests could cause one or both parties to run afoul of regulations under HIPAA. While the parties spend a good amount of time arguing this point, it isn't particularly relevant to this Court's consideration. HIPAA is complex legislation intended to ensure the privacy of any medium of information gathered by a covered entity during a patient's treatment. 42 U.S.C. § 1320d. The Department of Health and Human Services has promulgated regulations to assist patients and covered entities in interpreting HIPAA. *See generally* 45 C.F.R. § 164.500 *et seq.* The regulations provide that covered entities are not subject to HIPAA's requirements when acting pursuant to a court order or as part of an administrative proceeding. 45 C.F.R. § 164.512(e)(1).

While few opinions have been written in this arena, a review of existing cases convinces this Court that HIPAA should not obstruct the operation of the Federal Rules of Civil Procedure. *See e.g.* Shropshire v. Laidlaw Transit, Inc., No. 06-10682, 2006 WL 6323288 at 2 (E.D. Mich. Aug. 1, 2006) ("HIPAA regulations, while important, should be read in conjunction with the substance of the Federal Rules of Civil Procedure."); Bayne v. Provost, 359 F. Supp.2d 234, 237 (N.D.N.Y. 2005) ("Thus, under this specific rule and regulation, it is evidently denudate that a purpose of HIPAA was that health information, that may eventually be used in litigation or court

proceedings, should be made available during the discovery phase."). The undersigned has therefore reached a decision that is mindful of HIPAA's purpose but substantively based in the Civil Rules.

Having concluded that there are no statutory or contractual barriers, the undersigned turns to relevance and proportionality. The medical record is of course relevant to Plaintiff's claim that Dr. Smith was negligent in her treatment of Ms. Borum. Moreover, because Plaintiff claims that Deaconess was negligent in the management of its physician practice (DN 21 at PageID # 326-27), Plaintiff has demonstrated that the EMR system may be relevant as well. On the other hand, allowing Plaintiff to depose Dr. Smith while accessing the EMR system for the purpose of questioning her about her use of the software at the time of Plaintiff's treatment is unduly burdensome. Dr. Smith is being deposed about her care and treatment of Ms. Borum, not the EMR system. And, while her facility to use the system may be relevant to her ability to provide care, Plaintiff can gain an understanding of those matters through questioning. The potential for harassing or burdensome questioning by attempting to force Dr. Smith to perform a step-by-step reenactment of how she used the system at the relevant time outweighs any additional information that might be gained from such a demonstration. *See e.g.* Howard v. Michalek, 249 F.R.D. 288, 290 (N.D. Ill. 2008) (denying plaintiff's motion to compel security system monitor to reenact her movements at the police station, including zooming in on a particular holding cell); Jones v. Covington, 1:15-cv-396-WSD, 2015 WL 7721835 (N.D. Ga. Nov. 30, 2015) (denying a motion to ask a doctor to re-read a slide that the plaintiff alleged he had previously read incorrectly).

However, to enable Plaintiff to thoroughly depose Dr. Smith and to develop a complete understanding of Ms. Borum's medical record as it exists within the EMR system, Plaintiff will be allowed to perform an in person inspection of her medical record on the system itself. Additionally, Plaintiff requests an exact electronic copy of her medical record in its native format as well as the audit trail. Deaconess contends this is technically impossible (DN 19 at PageID # 277-78). But Plaintiff suggests in her response that, to the extent it in fact is impossible to produce an exact electronic copy, she will settle for printouts of the entire audit trail (DN 21 at PageID # 339-40). The Court assumes that Deaconess would not misrepresent the technological limits of its EMR system, and therefore orders that it provide Plaintiff with a printout of the entire audit trail.

2. Further Inspection of the EMR System and Creation of a Test Patient

Defendants additionally seek protection from Plaintiff's request that Deaconess allow Plaintiff to inspect its EMR system by having Deaconess create a fictitious “test patient” so that Plaintiff could manipulate that patient's record. Defendants again argue that creating a test patient would run afoul of HIPAA (DN 29 at PageID # 278). Furthermore, the Defendants argue any probative value of such an inspection would be greatly reduced or distorted because the system has been upgraded several times since 2015. Defendants also claim that, depending on how much information Plaintiff wished populated about the test patient, creating such a record could require a great deal of time and IT resources. Finally, Defendants claim that, because the test patient, if created, would not be allowed to access certain records, the accuracy and value of the inspection is eroded even further.

In response, Plaintiff contends Deaconess' advertisements stating that it is one of the most tech savvy hospitals in the region bely its claims that creating a test patient is somehow burdensome or infeasible (DN 21 at PageID # 345-46). Plaintiff further argues that setting up test patients is likely a routine part of training new employees and a process with which Deaconess' technical support personnel are already familiar. Finally, Plaintiff argues it is inequitable to require Plaintiff to hire an expert when Plaintiff's counsel could experiment with the EMR system on site. And, Plaintiff notes that Deaconess has customized the Epic system for its own use, and the only way to learn of these customizations is to use the system.

This is another relatively unexplored issue. In fact, the undersigned has been unable to locate a single case discussing access to EMR systems by counsel for purposes of assessing their functionality. However, the cases discussed above where a party seeks to compel another party to reenact or demonstrate something during a deposition are useful comparisons. The Sixth Circuit has not addressed the issue of compelling demonstrations in a deposition, but courts possess broad discretion to direct discovery. Waters v. City of Morristown, TN, 242 F.3d 353, 363 (6th Cir. 2001). Creating a test patient and entering hypothetical information about that patient is the functional equivalent of forcing Deaconess to reenact how its employees interacted with the EMR system when Plaintiff was a patient. By her own admission, Plaintiff seeks to create as exact a replica of the experience Dr. Smith would have had when Ms. Borum first presented for treatment (DN 21 at PageID # 346). The purpose of discovery is to learn facts that

already exist. Allowing the exploration of a test patient would instead create new facts not in existence at the time of Ms. Borum's treatment.[3] *See* Jones, 2015 WL 7721835 at 2. Plaintiff's request is therefore denied.

ORDER

IT IS HEREBY ORDERED that Defendants' motion (DN 19) is **GRANTED** in part and **DENIED** in part**.**

1. Defendants shall permit Plaintiff the opportunity to perform an on-site inspection of Plaintiff's EMR;

2. Defendants will provide Plaintiff a complete copy of Borum's EMR audit trail.

3. Defendants are not required to make the EMR system available during the deposition of Dr. Smith;

4. Defendants are not required to create a test patient in the EMR system for Plaintiff's experimentation.

H. Brent Brennenstuhl

H. Brent Brennenstuhl
United States Magistrate Judge

July 14, 2017

Copies: Counsel

[3] Plaintiff's attached state court order (DN 21 at PageID # 356) is not persuasive. First, the order contains no analysis of the issue. And even if it did, this case is governed by the Federal Rules of Civil Procedure, not the Kentucky rules. Fed. R. Civ. P. 81(c)(1).