**UNITED STATES DISTRICT COURT**
**DISTRICT OF CONNECTICUT**

| | | |
|---|---|---|
| **BARRY D. STEIN, BARRY D. STEIN, MD, LLC, and FAIRFIELD ANESTHESIA ASSOCIATIONS, LLC,** | : | **No. 3:19-cv-01634-VLB** |
| **Plaintiffs,** | : | **FEBRUANY 8, 2021** |
| **v.** | : | |
| **MELISSA J. NEEDLE, ESQUIRE, NEEDLE CUBA FIRM, THE LAW OFFICE OF MELISSA NEEDLE, LLC, JESSICA CALISE, AND JENNIFER STEIN** | : | |
| **Defendants.** | : | |

**ORDER AND DECISION ON ALLOCATION OF PAYMENT FOR COURT-APPROVED FORENSIC EXPERT**

**Before the Court is the issue raised in the parties' joint report; Dkt. 109; which is how payment to the court-approved computer forensic expert for his fees and costs should be allocated. The parties are on polar opposites. The Defendants arguing that the Plaintiffs should pay the entirety of the fees and the Plaintiffs arguing the reverse. The parties have submitted extensive briefing on this issue. *See* Def.'s First Memo of Law, Dkt. 113; Pl.'s First Memo of Law, Dkt. 114; Pl.'s Response, Dkt. 115; Def.'s Response, Dkt. 117; Pl.'s Reply, Dkt. 119. After careful review and consideration of the briefing along with the applicable legal standards and policies, the Court orders that the Defendants pay 100% of the computer forensic expert fees and costs.**

## I. BACKGROUND

**The underlying action was filed on October 16, 2019. Compl. Dkt. 1. In July 2020, the Plaintiffs filed the amended and now operative complaint. Am. Compl.,**

**Dkt. 73. In the amended complaint, Plaintiffs Barry D. Stein ("Dr. Stein") and Fairfield Anesthesia Associates, LLC ("FAA") allege that the Defendants—Melissa Needle ("Attorney Needle"), Needle Cuba Firm, the Law Office of Melissa Needle LLC (collectively the "Needle Firm"), Jessica Calise ("Calise"), and Jennifer Stein ("Mrs. Stein")—improperly accessed the Plaintiffs' home-computer and unlawfully copied private patient information from said computer. Am. Compl. at 2. Dr. Stein during relevant times was the owner and managing member of FAA, where he provided anesthesiology services to patients. Am. Compl. at ¶ 12. FAA maintains patient records on securely stored Microsoft OneDrive servers. *Id.* at ¶ 15. Dr. Stein owned and maintained a computer at his home on behalf of FAA. *Id.* at ¶ 17. The computer has two password-protected accounts, one for Dr. Stein and one for his wife Mrs. Stein with whom he lived with. *Id.* at ¶ 18. On Dr. Stein's home-computer sub account, he had access to FAA patient information through Microsoft OneDrive. *Id.* at ¶ 21.**

**Mrs. Stein filed for divorce on April 16, 2018.[1] According to the Connecticut Superior Court docket report, this divorce action is pending and is currently scheduled for trial in April 2021. Mrs. Stein states in a December 4, 2020 affidavit that in April 2018 she "used a password, which was known to me and shared within my family's household, to access [Dr. Stein's] Microsoft Windows user sub-account on a desktop located and used by me and other family members in the family home." Mrs. Stein Aff. at ¶ 3, Dkt, 113. She accessed Dr. Stein's sub-account**

**[1] The Court takes judicial notice of the Connecticut Superior Court docket report for case number FST-FA-18-6035933-S, showing that a divorce complaint was filed by Mrs. Stein on April 16, 2018.**

**and allowed Calise—who was a paralegal of her divorce lawyer Attorney Needle—to copy files from Dr. Stein's sub-account onto an external hard drive owned by the Needle Firm. Calise Aff. at ¶ 3, Dkt. 113. Calise then left the home, taking with her the external hard drive with the copied data. *Id.* at ¶ 4. When later reviewing the data on the hard drive, Calise found that she copied medical information related to Dr. Stein's patients. *Id.***

**The Plaintiffs brought the underlying action asserting a violation of the Computer Fraud and Abuse Act under 18 U.S.C. § 1030 *et seq.* against all Defendants, violation of the Connecticut Statutes under Connecticut General Statutes §§ 53-451 and 452 against all Defendants, negligence against all Defendants, and negligent supervision against Attorney Needle and the Needle Firm. Am. Compl. The Plaintiffs seek both injunctive relief and damages. *Id.***

**On October 28, 2020, Plaintiffs' counsel filed a letter to the Court requesting the immediate appointment of a neutral expert to conduct a forensic examination on the Needle Firm computer network. Ltr, Dkt. 100. In this letter, Plaintiffs state that in January 2020 they requested an inspection by an independent and agreed upon expert of the Needle Firm server, which was denied. *Id.* at 3. The letter further explains that FAA sent a notice of the United States Department of Health and Human Services ("HHS") reflecting the breach, to which HHS counsel directed FAA to undertake a media notification and notify all affected patients within 60 days. *Id.* FAA claims that in order to undertake this effort, it must ascertain the actual breadth and scope of the Defendants' exfiltration. *Id.* at 3–4. The letter provides**

**that the parties met on this issue and were unable to reach an agreed upon resolution. *Id.* at 4.**

**On October 30, 2020, the Court held a telephonic discovery dispute conference addressing the Plaintiff's letter. Following that conference, the Court entered the following order:**

> **The parties are ordered to meet and confer, then propose to the Court three computer forensic experts. The Court will choose one of the experts to serve as a special master tasked with examining the computer data of the Needle Firm and Dr. Stein's matrimonial counsel. In this examination, the special master will be required to identify any patient and employee information downloaded from Dr. Stein's FAA issued computer, identify whether such information was downloaded and stored, determine whether it was further disseminated, and if so, where. After receiving appropriate relief from the Superior Court, the special master will be required to validate or execute the permanent deletion of the confidential patient and employee information.**

**Order, Dkt. 105.**

**On November 18, 2020, the parties submitted a joint report concerning the computer forensic expert. Joint Report, Dkt. 109. In the joint report, the parties informed the Court they were able to reach an agreement on a single expert, John Clingerman. *Id.* The parties then included brief arguments that the other party should have to pay for the expert fees and costs. *Id.* The Plaintiffs' position was that "the fees and costs charged by the expert should be paid by Defendants who have acknowledged the downloading of the PHI from Plaintiffs' computer system." *Id.* The Defendants' position was that "the copying of the patient data was inadvertent and was the result of the Stein family computer lacking sufficient protections to prevent unauthorized access of HIPPA protected information." *Id.***

**The Court approved the computer forensic expert agreed upon by the parties. Order, Dkt. 110. The Court ordered the parties to submit supplemental briefs on the issue relating to expert fees, where the parties were to include affidavits supporting factual allegations. *Id.***

**The Defendant's first memorandum of law on this issue argued that the Plaintiff should bear the cost because Dr. Stein failed to implement sufficient protections to protect the patient information and the Defendants did not know, and had no reason to know, that the information copied contained patient information. Def.'s First Memo, Dkt. 113. In support of these allegations, the Defendants submitted affidavits from Mrs. Stein and Calise. *Id.* In Mrs. Stein's affidavit she admits to using Dr. Stein's password to access his sub-account on the home-computer, which allowed Calise to copy the data, but claims that Dr. Stein's password "was known to me and shared within my family's household." Mrs. Stein Aff. at ¶ 3. She states she entered a single password to access the sub-account. *Id.* at ¶ 4. She states she accessed the account because she did not trust Dr. Stein and believed he was manipulating the family's finances in a manner intended to keep her from benefiting in the divorce. *Id.* at ¶ 5. She cited to a "Bahamian trust" that Dr. Stein allegedly "transferred all of the marital assets, with the exception of the marital home, to . . . ." *Id.* Lastly, she states she was not looking for patient information. *Id.* at ¶ 6. In Calise's affidavit she states that she went to the Stein home, Mrs. Stein entered a password to access the computer, Calise reviewed the files on the computer and copied files onto an external hard drive. Calise Aff. at ¶ 3. Thereafter, Calise reviewed the data on the external hard**

**drive and discovered patient information. *Id.* at ¶ 4. In April 2019, in response to a request for production, she sent a Dropbox link to Dr. Stein's matrimonial counsel of the copied documents. *Id.* at ¶ 5.**

**The Plaintiff's also filed a first memorandum of law on this issue where it argues, *inter alia*, that the Defendants are totally culpable because Dr. Stein did not give Mrs. Stein his password nor did he give her authorization to access his sub-account. Pl.'s First Memo, Dkt. 114. In support of this memo, the Plaintiffs attach an affidavit from Dr. Stein where he states that at no time did he give Mrs. Stein his password or PIN. Dr. Stein Aff. at ¶ 9, Dkt. 114-5. Dr. Stein further states that "[a]ny access of the Protected Area by any of the Defendants in this action was done without my authorization, or the authorization of FAA, whether express or implied." *Id.* at ¶ 14.**

**The Plaintiffs filed a response to the Defendant's first memorandum of law where it states that the patient information was not stored locally on the computer, rather it was accessible only through a file labeled "FAA," meaning the Defendants' claim that they had no reason to know the files being downloaded were patient data, is illogical. Pl.'s Response, Dkt. 115. The Plaintiffs also claim that Mrs. Stein's discussion about the "Bahamian Trust" in her affidavit is "demonstrably false and misleading" because the statement gives the impression that this trust was created suddenly without her knowledge, when in fact she was involved in the process. *Id.***

**The Defendant filed a response to the Plaintiffs' first memorandum of law where they state that Dr. Stein made the decision to use a shared computer instead of a dedicated work computer, that there is evidence that the password was shared,**

**and the method of accessing the data should have included more protections such as two-factor authentication. Def.'s Response, Dkt. 117. The Defendants also argue that the Plaintiffs' attack on Mrs. Stein's statements relating to the Bahamian Trust misconstrues her statement because she never said that the trust was formed suddenly or without her knowledge, rather that Dr. Stein structured the trust in a way that she did not know or consent to. *Id.* The Defendants also included a text message exchange from August 29, 2016 between Dr. Stein and Mrs. Stein to support their claim that the password was shared. *Id.* at Ex. A. The exchange is as follows:**

> **[Mrs. Stein:] What's my outlook or your administrative password!**
> **[potential password #1] no work**
> **[Dr. Stein:] To log in to computer?**
> **[Mrs. Stein:] Yes – Eric installing software**
> **[Dr. Stein:] I think admin PW is [potential password #2]**
> **[Mrs. Stein:] Nope**
> **[Dr. Stein:] [potential password #3]**
> **[Mrs. Stein:] Nope**
> **[Dr. Stein:] [potential password #4]**
> **[Mrs. Stein:] Thank you**
> **[Dr. Stein:] Whew!**

***Id.***

**The Plaintiffs filed a response to the Defendants' response attaching an affidavit from Roney Manjoney, the technology consultant for FAA, who states that the above text message exchange relates to a password for the shared family account that controls the restrictions to their sons' (one of which is named Eric) computer. Roney Aff., Dkt. 121-1. Dr. Stein submitted an affidavit confirming this information as well. Dr. Stein Second Aff., Dkt, 121-2.**

## II. LEGAL STANDARD

**Federal Rules of Civil Procedure 26(b)(1) provides that:**

> **Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding 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 in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.**

**Rule 26(b)(2) carves out a special rule for electronically stored information, which authorizes a party not to provide electronically stored information that is not reasonably accessible because of undue burden or cost. However, the rule does provide that a "court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C)." Rule 26(b)(2)(B). "The court may specify conditions for the discovery." *Id.* Rule 26(b)(2)(C) requires courts to limit frequency and extent of discovery where it is unreasonably cumulative or duplicative, can be obtained by other less burdensome sources or less expensive, the requesting party has ample opportunity to obtain the information by discovery in the action, or the proposed discovery is outside the scope permitted under Rule 26(b)(1). Rule 34(a) authorizes a party to serve on any other party a request within the scope of Rule 26(b) to permit access to inspect electronically stored information.**

**Rule 53 governs the appointment of special masters. Subsection(g)(3) provides that "The court must allocate payment among the parties after considering the nature and amount of the controversy, the parties' means, and the**

**extent to which any party is more responsible than other parties for the reference to a master."**

**In *Genworth Financial Wealth Management, Inc. v. McMullan*, 267 F.R.D. 443 (D. Conn. 2010), this Court had cause to hear a somewhat analogous case. In *Genworth*, the plaintiff's former employees—the defendants—were accused of copying client data from the plaintiff's client database for the purpose of opening a competing business entity. *Id.* at 445. The defendants claimed they did not take this information, rather they formed their database based on internet searches and their memory. *Id.* The Court rejected this argument finding that the defendants were not telling the truth based on the evidence presented. *Id.* at 445–46, 448. The plaintiff in *Genworth* requested Court intervention to appoint a computer expert to forensically image and examine the contents of the defendants' computers, which the Court granted. *Id.* at 445. In determining who will pay the expense for this expert, the Court discussed both the defendants' alleged inability to pay and the "apparent deceit, obstreperousness, and destruction of relevant information" that necessitated the retention of the expert. *Id.* at 448. The Court ultimately ordered the defendants to pay 80% of the fees and the plaintiffs to pay 20% of the fees.**

## III. ANALYSIS

**The conduct alleged in this case is largely undisputed. Mrs. Stein admits to using Dr. Stein's password to enter his password-protected sub account and does not dispute that this access was without his knowledge or consent. The colloquy between the Steins wherein Dr. Stein gave Mrs. Stein his passcode to allow software to be installed on the computer confirms that Dr. Stein did not share his**

**passcode. Mrs. Stein admits her motivation was to access information accessible from only Dr. Stein's sub account. Calise admits downloading files onto an external hard drive that was found to contain Dr. Stein's patient's health information.**

**A forensic computer expert was approved to identify any patient and employee information downloaded from Dr. Stein's FAA issued computer, identify whether such information was downloaded and stored, determine whether it was further disseminated, and if so, where. Answers to these questions are necessary to provide the patients with notice of the full circumstances and extent of this breach. The public has deemed patient health information to be a significant privacy interest, evidenced by the substantial regulations, by both state and federal authorities, protecting this information.[2] The patient's interest in their health information greatly outweigh any interest the Defendants have in this case. This is why the Court previously authorized the appointment of a neutral computer expert.**

**With that said, the Court must determine who should be responsible for paying for this expert at this stage.[3] The Court finds persuasive the Plaintiffs' arguments and unpersuasive the Defendants'.**

---

**[2] Including the Health Insurance Portability and Accountability Act of 1996 (HIPPA), 42 U.S.C. § 1320d, *et sea.*; Connecticut General Statues § 52-146o (generally prohibits disclosure of patient communication or information by physician, surgeon or healthcare provider); federal regulations under Title 45 of the Code of Federal Regulations.**

**[3] This allocation may be amended once a decision on the merits is rendered. *See* Rule 53(g)(3).**

**Contrary to the Defendants' position, the Court finds that Dr. Stein and FAA did take the necessary steps to protect patient information. It is undisputed that the only way to access the patient information was by accessing Dr. Stein's sub account, which was accessible only by using his password. Based on the affidavits of FAA's technology consultant, Manjoney, the purpose of having separate accounts was to protect this very information. Manjoney attests through his employment with FAA he installed and configured Dr. Stein's home-computer to be in compliance with HIPPA guidelines and set up separate sub accounts. Manjoney Aff. at ¶ 9. This included a password protected sub account for Dr. Stein. *Id.* Manjoney also set up sub accounts for the other family members, meaning that when they used the home-computer they would have no need to access Dr. Stein's sub account. *Id.* at ¶ 10.**

**The Defendants' claimed evidence that Dr. Stein "shared his passwords on occasion, including passwords to the family desktop at issue in this case" miss construes the issues here. Whether he shared a password unrelated to his patient's health information is of no consequence here. The issue here is whether he both shared the password to his sub-account where the information is sought and whether he authorized the access of his patients' health information. The text message exchange provided by the Defendants does not exhibit this. The text messages simply show that Dr. Stein provided Mrs. Stein with a password for the purpose of allowing their son Eric to install software. The password was not given for the purpose of authorizing Mrs. Stein to use it eighteen months later to remove his data, including his patient's health data.**

**Further, when Dr. Stein send this text message, he and Mrs. Stein were married. The law commonly recognizes the importance of protecting marriage communications, commonly known as the marital communications privilege, which "encourages married people to confide in each other" and "feel free to communicate" with each other. *State v. Davallo*, 320 Conn. 123, 140 (2016). Connecticut statute protects the "confidential communication," with exception, "made between spouses during a marriage that is intended to be confidential and is induced by the affection, confidence, loyalty and integrity of the marital relationship." Conn. Gen. Stat. § 54-84b(a). While these principles do not directly apply here, the policies behind these principles do. Even if Dr. Stein gave Mrs. Stein a password to his sub account the colloquy makes clear he maintained the data under password protection from others who used the computer and divulged it solely to allow software to be installed. He shared this confidential information when the parties were still married. Her subsequent use of the password in the way she used it was not only unauthorized; it was in betrayal of the marital trust.**

**Mrs. Stein's intentions in authorizing the copying of the patient information does not provide a basis for avoiding responsibility for paying the computer forensic expert who is necessary solely due to her conduct. The Court finds Mrs. Stein or Calise claim that they did not realize they were copying information relating to over 800 patients questionable, particularly since Calise attests that she did, *albeit* very briefly, review the files being copied. Mrs. Stein authorized, at the very least, the negligent duplication and disbursement of health information of over 800 people. Further, the argument that Dr. Stein should have had a second password**

**to access the patient information is of no avail. It is the equivalent of a burglar blaming a homeowner for not locking away jewelry when the front door was locked. Mrs. Stein did not have authority to enter in the first instance.**

**Further, Mrs. Stein's motivations in authorizing the copying of patient health information does not provide a basis for avoiding responsibility for paying for the computer forensic expert who is necessary solely due to her conduct. There is no evidence presented that she could not have accessed this information through legal means. She was represented by counsel who should know the rules of discovery and the avenues for avoiding electronic spoliation. Instead of exercising her legal rights in order to protect and obtain access to this information in her divorce proceedings, she took it amongst herself to access Dr. Stein's sub account and authorize the copying of his information, which included the copying of the protected health information of over 800 other people.**

**In comparing this case to *Genworth*, where the Court ordered defendants to pay 80% of the fees and the plaintiff pay 20%, the justification for requiring the plaintiff to pay anything are not present here. In *Genworth*, the defendants asserted an inability to pay the expense for the expert. Here, the Defendants have not asserted an inability to pay.**

**Therefore, because the Court finds that the Defendants are solely responsible for the need for an computer forensic expert in this case and no other mitigating factor justifies requiring the plaintiff to pay some of the expert fees, the Court orders that the Defendants are 100% responsible for the computer expert fees and costs at this time.**

## IV. CONCLUSION

**For the above reasons, the Court orders the Defendants to pay 100% of the court-approved computer expert fees to the extent that the fees are incurred while the expert is operating within the scope of the expert's responsibilities as laid out in the Court's order. Dkt. 105.**

**IT IS SO ORDERED.**

**/s/**
**Hon. Vanessa L. Bryant**
**United States District Judge**

**Dated this day in Hartford, Connecticut: February 8, 2021**