New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 254—NO. 43
TUESDAY, SEPTEMBER 1, 2015

State E-Discovery

Medical Malpractice E-Discovery, Preservation and Privilege Logs

By **Mark A. Berman**

Medical malpractice counsel are seeking more sophisticated e-discovery, with plaintiffs, as in *Vargas v. Lee*,[1] wanting to discover physicians and hospitals' electronic medical records (EMR) along with their attendant electronic "audit trails." This is a relatively nascent area of e-discovery with few decisions issued on it.[2] On the defense side, in *Angel v. Rubin*,[3] a physician's counsel also became more sophisticated and sought patient emails and text messages attempting to refute claims of alleged deficient medical care. Electronically stored information (ESI) court stipulations are now de rigueur in commercial cases and compliance with them, and the proper submission of a privilege log identifying emails allegedly protected from disclosure by privilege or the work product doctrine, are required as noted in *Herman v. Herman*.[4] Storage of ESI in the "cloud" may not serve as a basis to assert lack of "possession, custody or control" over ESI, even if the vendor agreement governing "cloud" storage ended as in *S.R.E.B. v. E.K.E.B.*[5] Finally, in *Baron v. Black*,[6] no spoliation sanction was issued where the deletion of emails by plaintiff allegedly occurred only because Google notified him that emails needed to be deleted to free up space in his company's Gmail account.

BIGSTOCK

Electronic Medical Records

In *Vargas*, a medical malpractice action concerning post-surgical complications, at issue was the production of the "audit trail" of the hospital's EMRs. Plaintiff asserted that the "audit trail" would provide material and necessary information regarding the timing and substance of plaintiff's post-surgical care. The motion court noted that the "issue of metadata production is at the forefront of present day e-discovery disputes." Nevertheless, the court held that "plaintiff has not distinguished the audit trail's utility from that of its corresponding EMR" where plaintiff could presumably obtain the patient's treatment details from the already produced EMRs. The court noted:

> In some instances, system metadata production has been considered relevant when the process by which a document is created is in issue or there are questions concerning a document's authenticity. While not a prerequisite to meta-data production, such authenticity issues speak to the utility and necessity of such production. Here, plaintiff does not articulate any analogous or salient consideration. General comments that the audit trial may provide discovery on the "timing and substance of plaintiff's care" are insufficient.

As such, the motion court held that "plaintiff has not satisfied his burden of establishing the necessity and utility of audit trail production." Accordingly, the motion to compel was denied without prejudice to renewal upon a proper showing.

Patient Emails and Text Messages

In *Angel*, a medical malpractice action, defendant physician moved for an order compelling discovery of "non-privileged communications, including phone records (home and cell), emails, and text messages limited to the 14 or 16 hour period after the decedent was seen by" defendant. The physician asserted that his notes indicated that he advised plaintiff to go to the hospital, but that plaintiff refused, and that plaintiff's communications from that visit to his death would shed light on this contention and refute decedent's wife's testimony that the physician not only did not tell him to go to the hospital, but actively dissuaded him from doing so. The motion court granted the motion where decedent was unavailable to testify on this "critical" issue.

ESI Cloud Preservation

In *S.R.E.B.*, a wife contended that her husband had been video recording in the home and that he records continuously with two permanently affixed "DropCam" cameras that are equipped with motion detectors, night vision, and high audio capture ability, which transmit and store recordings on an online cloud for seven to 30 days. The husband contended that he had produced video files stored on an Internet cloud (to which his wife did not have access) to the

---

MARK A. BERMAN, *a partner at commercial litigation firm Ganfer & Shore, cochairs the social media committee of the Commercial and Federal Litigation Section of the New York State Bar Association.*

extent that they were under his "custody and control." However, the husband failed to address "whether or not he retained the audio and video [files] after the subpoenas were served upon him" and "whether or not he allowed the audio and video files to lapse and automatically be deleted from the cloud each period so as to purposefully relinquish control over the material." The motion court noted that the husband's claim that he was unable to obtain certain records is "unconvincing in a day and age where cloud storage allows for convenient and extensive access" and that "[e]ven if the files were not under the husband's custody or control, he was bound to take the steps necessary to assure their preservation" given the notice provided to him in the Preliminary Conference Order. The motion court found that the husband's claim that he was "unable to obtain the requested audio and video files [was] completely unavailing [based] upon the fact that he [was] able to store files from the cloud, make the files independent from the cloud, and thereby [had] access to them after the cloud access period has lapsed." Finally, the above demonstrated to the court that "there were steps available to the husband to assure the preservation of the material."

Privilege Logs and Preservation

In *Herman*, 10 months after the action was commenced, the parties agreed to a preservation stipulation which provided:

> [f]or the relevant periods relating to the issues in this litigation, each party shall take all reasonable steps (including suspending aspects of ordinary computer processing and/or backup of data that may compromise or destroy [ESI]), necessary to, maintain and preserve such ESI as may be (i) relevant to the parties' claims and/or defenses, or (ii) reasonably calculated to lead to the discovery of admissible evidence, including but not limited to all such ESI data generated by and/or stored on the party's computer system(s) and/or any computer system and storage media (i.e., internal and external hard drives, hard disks, floppy disks, memory sticks, flash drives and backup tapes), under the party's possession, custody and/or control. The failure to comply herewith may result in appropriate sanctions or such other relief as the court may be authorized to impose or award, including but not limited to precluding use of evidence, taking adverse inferences, and/or rendering judgment in whole or part against the offending party(ies).

Notwithstanding the preservation stipulation, the motion court held that even before it was executed, defendant "had an obligation to preserve ESI, since the obligation to preserve ESI begins when litigation is reasonably anticipated." Further, the motion court noted that the destruction of ESI after litigation begins is "grossly negligent, if not intentional." Ultimately, the motion court concluded that defendant wrongfully deleted certain emails in violation of his obligation to preserve ESI and directed there to be an adverse inference based upon defendant's failure to deny that he had deleted such emails.

The motion court also found that defendant had failed to serve an appropriate privilege log with respect to certain emails. The court noted that a list of bates numbers without any description and only containing notations as to whether counsel had agreed to production or was asserting a right to redact or withhold entirely on the grounds of attorney-client or work product privilege violated the court's compliance order. The motion court also held that it did not comply with CPLR Rule 3122, Commercial Division Rule 11-b, "which suggests categorical logging of documents," or the court's individual practice rule regarding logging of privileged documents, which requires that with a response to a document demand "the party asserting the privilege shall serve on all other parties a privilege log of the responsive documents that are not being disclosed and a copy of the redacted documents, bate-stamped. The privilege log shall identify all redacted and completely withheld documents by bate-stamp numbers, dates, authors and recipients, the general subject matter of the document if it will not waive the privilege, and shall state the privileges being asserted."

> In 'Baron,' no spoliation sanction was issued where the deletion of emails by plaintiff allegedly occurred only because Google notified him that emails needed to be deleted to free up space in his company's Gmail account.

Spoliation Sanctions Denied

In *Baron*, plaintiffs commenced their action alleging causes of action for slander, libel, tortious interference with economic advantage, abuse of process, false arrest and false imprisonment, negligence and gross negligence and intentional infliction of emotional distress arising out of alleged false statements made by the defendant about the individual plaintiff. Defendant sought, inter alia, to dismiss the complaint resulting from the spoliation of evidence. The motion court found that the defendant failed to establish that plaintiffs' conduct rose to the level of spoliation. At his deposition, plaintiff testified that he and the faculty at the Fashion Institute of Technology (FIT) emailed about his alleged hire and that he previously applied for a job with FIT, but that he was rejected and notified about said rejection by email. The plaintiff also testified that he recently deleted thousands of emails from his company's Gmail account without producing them for defendant's review during discovery. The above testimony served as the predicate for defendant's motion asserting that certain emails regarding plaintiff's alleged employment with FIT were not provided during discovery and thus defendant "can only suppose that these were among many other relevant documents that [plaintiff] intentionally deleted."

The motion court noted that "[a]s an initial matter, defendant has not established that plaintiffs had an obligation to preserve the deleted emails as there is no evidence that the emails were relevant to the instant action." The motion court held:

> Defendant has not established that plaintiffs deleted the emails with a "culpable state of mind." Indeed, plaintiffs have affirmed that the emails were deleted only after receiving a notification from Google that emails needed to be deleted in order to free up space in plaintiff's Gmail account and defendant has not presented any evidence that the emails were deleted for any other reason. Finally, defendant has not established that the deleted emails were relevant to defendant's defense in the instant action. While defendant asserts that the deleted emails likely involved plaintiff's alleged employment with FIT, plaintiff Baron has affirmed that he deleted thousands of emails but that he "did not delete any emails that are relevant to this litigation." Specifically, plaintiff Baron affirmed that he "specifically did not delete any emails that related to: (1) the Defendant Seven Black; (2) the 'Fashion Institute'; and (3) '315 Seventh Avenue'" and that he has provided defendant with any and all discovery related to his alleged employment with FIT.

••••••••••••●●●••••••••••••••

1. 2015 NY Slip Op 31048, 2015 N.Y. Misc. LEXIS 2176 (Sup. Ct. Kings Co. June 10, 2015).

2. See Justice John M. Curran and Mark A. Berman, "Gremlins and Glitches: Using Electronic Health Records at Trial," New York State Bar Association Journal, May 2013, Vol. 85 No. 4. See *Karam v. Adirondack Neurosurgical Specialists, P.C.*, 93 A.D.3d 1260, 941 N.Y.S.2d 402 (4th Dept. 2012) (counsel for defendants "attempted to introduce an "audit trail" of the computer system establishing that much of the 11:23 a.m. note was made at a later time … . The court denied defendants' request to allow evidence of the audit trail and for a mistrial and declined to impose sanctions."); *Pamphile v. Queens-Long Island Med. Grp., P.C.*, Index No. 2431/2014 (Sup. Ct. Nassau Co. Dec. 22, 2014) (denying the production of the "audit trail" of electronic medical health records). See also *American Express Centurion Bank v. Badalamenti*, 30 Misc. 3d 1201(A), 958 N.Y.S.2d 644 (Dist. Ct. Nassau Co. 2010) (electronically stored images "cannot qualify as a reproduction of an original made in the ordinary course of business unless the enterprise in question has incorporated into its technology security measures sufficient to guarantee that any such alteration leaves an *audit trail* which at least indicates that a change has been made") (citation omitted and emphasis added).

3. 2015 NY Slip Op 31369(U), 2015 N.Y. Misc. LEXIS 2653 (Sup. Ct. N.Y. Co. July 17, 2015).

4. 2015 NY Slip Op 31205(U), 2015 N.Y. Misc. LEXIS 2447 (Sup. Ct. N.Y. Co. July 13, 2015).

5. 2015 NY Slip Op 51158(U), 2015 N.Y. Misc. LEXIS 2869 (Sup. Ct. Kings Co. Aug. 6, 2015).

6. 2015 NY Slip Op 31201(U), 2015 N.Y. Misc. LEXIS 2432 (Sup. Ct. N.Y. Co. July 10, 2015).

Reprinted with permission from the September 1, 2015 edition of the NEW YORK LAW JOURNAL © 2015 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-08-15-43

GANFER & SHORE, LLP
ATTORNEYS AT LAW

360 Lexington Avenue
New York, New York 10017
212.922.9250
sshore@ganfershore.com