Lost Data and Its Implications for Litigation

Save to myBoK

By Ron Hedges, JD

Healthcare providers deal with electronic information on a daily basis. Providers must expect that volumes and varieties of electronic information will increase exponentially with, for example, the rise of artificial intelligence in the diagnosis and treatment of patients. That electronic information likely will be defined as electronic protected health information (ePHI) and fall within the definition of the electronic health record (EHR), although a provider will create, store, and maintain electronic information that may not be included in the EHR, such as nursing notes.

Whatever the format of the data and wherever it might reside within the information technology (IT) structure of a healthcare provider or within the structure of a business associate (BA), there may come a time when it must be located or retrieved, preserved, and produced for litigation-related purposes. When relevant electronic information is "lost," the provider who should have preserved it may be sanctioned. Courts across the country use different tests to determine whether sanctions should be imposed for the loss of electronic information or, as it is commonly known, electronically stored information (ESI). This article will look at the meaning of lost ESI under the Federal Rules of Civil Procedure. Examples of litigation in which ESI might be relevant include, for example, medical malpractice causes of action in which the content of the EHR might be used to prove or rebut an allegation of misdiagnosis or improper treatment.

What Does 'Lost' Mean?

Federal Rule 37(e) governs the imposition of sanctions for the loss of ESI. The rule authorizes sanctions if four conditions are met:

1. The ESI at issue should have been preserved in anticipation or conduct of litigation
2. The ESI is lost
3. The loss is due to a party's failure to take reasonable steps to preserve it
4. The ESI cannot be restored or replaced through additional discovery

This article focuses on the third condition.

"Lost" must be considered in context. Although not related to healthcare, *Franklin v. Howard Brown Health Center*, No. 17 CV 8376, 2018 WL 4784668 (N.D. Ill. Oct.4), report and recommendation adopted, 2018 WL 5831995 (N.D. Ill. Nov. 7, 2018), provides an example. The plaintiff in *Franklin*, which was an employment discrimination action, requested that the defendant produce emails and text messages to support the plaintiff's claim he had been harassed by the defendant's personnel. The plaintiff was actually seeking instant messages, the purported method by which he was harassed. The defendant produced two instant messages and could not produce any others. The plaintiff moved for the imposition of sanctions under Rule 37(e). Here are some of the findings of the court in ruling on the motion:

- The defendant's general counsel had issued an untimely and ineffective legal hold that gave "no indication what employees were to do with documents or electronic files and information that had to be preserved, or how they should be preserved, and there was no indication they should forward or deliver the information, files, etc., to defendant's legal department."

- No attorney supervised the preservation efforts of the defendant's employees. Rather, employees decided "on their own what was relevant and what wasn't."
- Additional instant messages had existed on a hard drive of a former employee of the defendant but the hard drive's data had been deleted.
- The plaintiff's work computer, on which the additional instant messages were presumably stored, could not be located even though it had been supposedly preserved.
- Any instant messages that had existed on the computers of the plaintiff's harassers—other employees of the defendant—had been autodeleted.

Based on these and other findings the court concluded that the defendant had been grossly negligent in its failure to preserve the additional instant messages and recommended that the parties "be allowed to present evidence and argument to the jury regarding the defendant's destruction/failure to preserve electronic evidence in this case, and that the jury be instructed as the trial judge deems appropriate."

In reaching its conclusion the *Franklin* court necessarily found that the ESI had been "lost" within the meaning of Rule 37(e). However, is the loss of ESI within a healthcare provider's IT systems self-evident when that ESI no longer resides within the system? *Envy Hawaii LLC v. Volvo Car USA LLC*, Civ. No. 17-00040 HG-RT (D. Hawaii Mar. 20, 2019) provides an answer.

Envy Hawaii arose out of a contract dispute and allegations of improper business practices between a Hawaiian car dealership and the national distributor of Volvos. After two years of litigation, which included document production and depositions, the defendants moved for sanctions against the plaintiff for its failure to preserve "Google e-mail accounts and electronic dealer management system records." The court denied the motion, finding that that ESI had not been lost.

The court began with a review of Rule 37(e): "The text of Federal Rule of Civil Procedure 37(e) provides that evidence is 'lost' and subject to spoliation sanctions when a party failed to take reasonable steps to preserve it, and 'it cannot be restored or replaced through additional discovery.'"

The court then focused on the meaning of "lost" under the rule: "Information is 'lost' for purposes of Rule 37(e) only if it is irretrievable from another source, including other custodians."

Moreover:

> Cases decided after the implementation of the 2015 amendment to Fed. R. Civ. P. 37(e) have highlighted the 2015 Advisory Committee Notes to the Rule. The 2015 Advisory Committee stated that "because electronically stored information often exists in multiple locations, loss from one source may often be harmless when substitute information can be found elsewhere." Fed. R. Civ. P. 37(e), 2015 Advisor [sic] Committee Notes.[1]

With this focus, the court turned to the facts before it and found that the defendants (the moving parties) had not met their burden to show that the ESI had been lost. The plaintiffs might not have preserved the ESI but the ESI might be stored with third parties, which maintained the ESI on behalf of the plaintiffs. Moreover, the court observed that the defendants had not subpoenaed the third parties for the ESI or attempted to retrieve it from a system to which they had access. Under these circumstances, the court concluded that the ESI had not been lost and left the defendants to serve subpoenas.

Implications for HIM

What lessons might *Envy Hawaii* have for a health information management (HIM) professional? There are several, all arising when the professional is called upon for assistance during litigation:

- The professional should consider where relevant information resides within the provider's IT system.
- The professional should understand whether relevant ESI resides outside the provider, for example, with a business associate or in the cloud.
- The professional should understand the need to preserve that ESI and, as directed by counsel, take steps to preserve the ESI. That necessitates a knowledge of the form in which the ESI was created and how it was stored so that relevant metadata can be preserved.

This role for the professional might exist whether or not the focus of preservation is solely the EHR or whether other ESI, as in the earlier example of nurse's notes, which might be the subject of preservation.

This means that the HIM professional may have a central role in avoiding the loss of relevant ESI.

Note: For a broader discussion of the role that the HIM professional can have in litigation see the AHIMA Practice Brief, "Health Information Management and Litigation: How the Two Meet," published in the May 2019 issue of the *Journal of AHIMA* and available online in AHIMA's HIM Body of Knowledge.

Note

1. Envy Hawaii LLC v. Volvo Car USA LLC. Civ. No. 17-00040 HG-RT. https://ediscovery.co/wp-content/uploads/2019/04/Envy-Hawaii-LLC-v.-Volvo-Car-USA-LLC_2019-04-01-06_32_20-0400.pdf.

Reference

Gotteher, Gail and Ron Hedges. "Using Information Governance to Avoid Data Breaches and Provide Cybersecurity." *Journal of AHIMA* 90, vol. 4 (April 2019): 30-31.

Ron Hedges (r_hedges@live.com), JD, is a former US Magistrate Judge in the District of New Jersey and is a writer, lecturer, and consultant on topics related to, among other things, electronic information. He is a senior counsel with Dentons US LLP.

Article citation:
Hedges, Ron. "Lost Data and Its Implications for Litigation" *Journal of AHIMA* 90, no.8 (August 2019): 34-35.