Spoliation of Medical Evidence

Save to myBoK

by Jonathan P. Tomes, JD

To avoid the improper destruction or alteration of records, HIM departments must follow a retention schedule, train personnel, and ensure that corrections leave original entries intact.

Although the legal concept known as spoliation of evidence has been a part of the American legal system for some time, including medical-legal litigation, the move toward the electronic health record (EHR) has increased the need for HIM professionals to understand spoliation, its consequences, and how to avoid it.

Spoliation is, quite simply, the "intentional destruction, mutilation, alteration, or concealment of evidence."[1] In the medical environment, spoliation is most likely to occur in the context of malpractice litigation. A healthcare provider or healthcare worker could destroy, alter, or conceal a medical record that may document possible malpractice. For example, in *Friedman Professional Management Co., Inc. v. Norcal Mutual Insurance Co.*, a doctor faced a malpractice action and both hid medical records and instructed his nurse to alter them.[2]

Courts have condemned spoliation. One court has recognized that "[b]asic to the administration of justice is the search for truth."[3] The search for truth breaks down, however, when parties do not have the opportunity to adduce all relevant evidence at trial.[4] The Supreme Court of California has noted that "spoliation . . . undermines the search for truth and fairness by creating a false picture of the evidence before the trier of fact."[5] Further, according to the same court, spoliation may leave the trial record incomplete, may affect the apparent relevancy of other evidence, and may increase litigation costs as litigants scramble to reconstruct the spoliated evidence or to develop other evidence, which may be less accessible, less persuasive, or both. Therefore, destroying evidence can destroy fairness and justice, for it increases the risk of an erroneous decision on the merits of the underlying cause of action.[6]

Courts should not be the only entities aghast at spoliation of medical evidence. Healthcare workers, particularly HIM professionals, must protect health information. The AHIMA Code of Ethics specifies that its members must take the following actions:

> III. Preserve, protect, and secure personal health information in any form or medium and hold in the highest regard the contents of the records and other information of a confidential nature, taking into account the applicable statutes and regulations.
>
> IV. Refuse to participate in or conceal unethical practices or procedures.[7]

How to Prevent Spoliation

Although the principles are similar, some differences exist with regard to preventing spoliation in paper records and in electronic ones.

Healthcare entities, whether large hospitals or small physician practices, should have a formal retention program for paper and electronic records. A retention schedule specifies how long the entity must preserve various types of records. Retention periods depend on legal requirements to preserve records, statutes of limitations (the time within which a lawsuit may be brought), and business and medical needs for the information. The retention schedule must, however, specify that, regardless of whether or not the retention period has expired, records that are involved in an outside audit, an investigation, or any litigation may not be destroyed. The entity *must* comply with its retention program. Destroying records pursuant to a proper retention program is not spoliation. Destroying records otherwise may be.

Next, entities must train all personnel on the dangers of destroying, altering, or removing records. Staff may think that they are being helpful by cleaning up files and removing what they think are duplicate, superfluous, or unnecessary records. They may think that they are saving the facility or the patient copying fees or other money by removing records marked as belonging to someone other than the patient and not part of the official medical record. Removing such files, however, could cost the facility hundreds of thousands of dollars in spoliation liability and even harm a patient.

Inaccurate entries are far more likely to result in a malpractice claim than spoliation is. Errors that are improperly corrected, however, can result in spoliation, also exposing the organization to risk. In correcting a record, the initial, incorrect information must always remain intact. When correcting paper records, "a single line should be drawn through the entry containing the error, the correct data should be recorded, and the individual making the correction should sign and date it. The original entry should never be obliterated."[8] The method is different for electronic records, but the principles remain the same.

Preventing Spoliation of Electronic Records

Although a good forensic computer expert can often recover data that have been deleted or overwritten, the law requires that EHRs be corrected in a similar manner to paper records—that is, by leaving the original entry intact. Professional standards call for the same treatment: "For errors corrected in a computer-based record, the system should preserve both the original entry and the amendment, as well as the identity of the person making the amendment and the date and time it was made."[9]

This guidance is consistent with HIPAA. Although no section of HIPAA or its implementing security and privacy rules sets out how to correct an EHR, a number of sections provide guidance. Although the final security rule did not include the electronic signature standard, the draft standard specifies that an electronic signature must include message integrity, nonrepudiation, and user authentication.[10]

If the electronic signature standard is finalized, it will probably include these three implementation specifications. The message integrity standard supports the proposition that the entry must be accurate and not corrected in a manner that fails to preserve the incorrect data. Nonrepudiation is the ability to authenticate the sender (or signer) of a message and its contents. An improper correction that does not identify the party making the correction violates the nonrepudiation requirement.

The final security rule, however, does include the following specifications:

- Information system activity review, which requires auditing records for accuracy, security, and so forth[11]
- Unique user identification, which allows the entity to identify and track user identity, such as who made a correction[12]
- Audit controls, which are the technical component of information system activity review[13]

The two standards of the security rule that most clearly require proper correction of the EHR are the integrity standard and the transmission security standard. The former requires covered entities to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.[14] The transmission security standard's integrity controls implementation specification requires security measures to ensure that transmitted electronic protected health information is not improperly modified without detection until disposed of.[15]

Whether the provider is a covered entity that must comply with the HIPAA security rule or not, following these implementation specifications will go a long way toward preventing spoliation of EHRs. Spoliation can clearly harm healthcare entities and their patients. Both the law and professional standards make spoliation improper, and the law has developed sanctions for those who commit spoliation. Healthcare providers can avoid spoliation by following a retention schedule, including a prohibition on destroying records that may be involved in audit, investigation, or litigation. They must also train staff on the proper retention and correction of health information, ensuring that any corrections, whether on paper charts or in an EHR, leave the original entry intact.

How Attorneys Search for Spoliation

Upon getting a new case, a malpractice attorney might first ask the alleged malpractice victim to obtain a copy of his or her complete medical record from the provider. The attorney might next have the new client sign a proper authorization for release of health information and then request a copy

of the complete medical record on law firm letterhead accompanied by the authorization. The third step would be to compare the two copies—if they are different, the provider may have culled out documents that it believed would show malpractice, thus committing spoliation. Finding spoliation is a malpractice attorney's dream.

In the final step, the attorney might have a nurse legal practitioner review the record to determine whether the provider properly charted the patient's care. The practitioner would likely focus on issues regarding incomplete or altered records: whether each record belongs to the patient, whether the record contains gaps, whether the record has unexplained alterations, and whether discrepancies appear among various records. Only after this complete analysis of the record would the attorney retain medical expert witnesses to opine whether the record indicates that malpractice occurred.[1] Thus healthcare entities must not only ensure the completeness and accuracy of medical records to avoid malpractice exposure, but also ensure that no staff member commits spoliation.

Note

1. See *generally* Jonathan P. Tomes, *How to Review Medical Records in Illinois*, Illinois Institute for Continuing Legal Education (1991).

How Courts Punish Spoliation

The law does not rely solely on codes of ethics and honest healthcare workers to prevent spoliation, of course. Consequently, the law has developed a number of sanctions for spoliation of evidence, including a separate lawsuit for spoliation, discovery sanctions, and jury instructions that jurors may consider that the missing or altered evidence is adverse to the party who concealed or altered the record.

Not all states recognize a separate lawsuit for spoliation of evidence. Among those that do are Alaska, California, Kansas, Ohio, New Mexico, and Florida. The District of Columbia, North Carolina, and New Jersey recognize torts analogous to spoliation, and New York recognizes a cause of action "where a plaintiff can establish with some evidence that a defendant has intentionally destroyed materials with the intention of obstructing a potential third party claim."[1]

A court may impose discovery sanctions against a party who commits spoliation. Under Federal Rule of Civil Procedure 37(b)(2)(A)-(E), for example, the court may take certain facts as given, refuse to hear certain claims or defenses, refuse to admit certain evidence, strike certain pleadings, stay or dismiss part or all of the action, render judgment by default, hold the violator in contempt of court, or take action based on any logically consistent combination of the above. Additionally, under rule 37(b)(2), the court may force payment of certain costs and attorneys' fees. For example, the federal court in *Trigon Ins. Co. v. United States* awarded nearly $180,000 in attorneys' fees and expenses as a sanction for spoliation of evidence.[2] In another federal case, the court imposed a $1 million sanction for failure to prevent the destruction of electronic data.[3] All of these sanctions could be devastating in a medical malpractice case.

In *Keene v. Brigham and Women's Hospital*, Keene brought a medical malpractice action against Brigham and Women's Hospital.[4] The hospital failed to produce all of Keene's medical records, and Keene moved for a default sanction against the hospital. The Supreme Judicial Court held that the Superior Court judge had acted properly by imposing a default sanction against the hospital on the issue of liability under the doctrine of spoliation for failure to produce medical records. Thus, the defendant hospital had no opportunity to present any defenses on the issue of liability.

Finally, a court may instruct the jury that it may infer that the destroyed or altered evidence was adverse to the party committing the spoliation. In *Banks ex rel. Banks v. Sunrise Hospital*, a malpractice case involving allegedly defective anesthesia equipment, the hospital failed to document which equipment had been used in the plaintiff's operation.[5] The court did not find that the hospital had willfully disposed of the equipment to frustrate the plaintiff's discovering evidence that the machine used was defective; however, it did instruct the jurors that they could infer that, if the anesthesia equipment used in the patient's surgery had been preserved and tested, it would have been found to be not operating properly. The Supreme Court of Nevada upheld this sanction for spoliation of evidence. Such an inference would be almost impossible to overcome without producing the actual machine used and demonstrating that it performed properly.

Notes

1. Sara D. Guardino and Lissy C. Friedman. "Remedies for Document Destruction: Tales from the Tobacco Wars," 12 *Virginia Journal of Social Policy and the Law* 1 (Fall 2004).
2. CIV.3:00CV365, 2002 WL 3184265 (E.D. Va. 2002).
3. *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 617 (D.N.J. 1997).
4. 439 Mass. 223, 235 (2003).
5. 102 P.3d 52 (Nev. 2004).

Notes

1. Black's Law Dictionary (8th ed. 2004). *See Hannah v. Heeter*, 213 W.Va. 704, 584 S.E.2d 560 (W.Va. 2003).
2. 120 Cal.App.4th 17, 15 Cal.Rptr.3d 359 (Cal.App. 4th Dist. 2004).
3. *Page v. Columbia Natural Resources, Inc.*, 198 W.V2.378, 480s.E.2d817, 825 (1996).
4. *Id.*
5. *Cedars-Sinai Medical Center v. Superior Court*, 18 Cal.4th 1, 9, 74 Cal.Rptr.2d 248, 253, 954 P.2d 511, 516 (Cal. 1988).
6. Id. at 954 P.2d at 515.
7. AHIMA Code of Ethics. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.
8. HIMSS. CPRI Toolkit: Managing Information Security in Health Care. 2003. Section 5.2. Available online at www.himss.org/CPRIToolkit/html/5.2.html.
9. *Id.*
10. Proposed Rules, Department of Health and Human Services, Draft Regulations on the Security of Individual Health Information, 45 C.F.R. Part 142, E., Electronic Signature Standard.
11. 45 C.F.R. § 164.308(ii)(D).
12. 45 C.F.R. § 164.312(a)(2)(i)
13. 45 C.F.R. § 164.312(b).
14. 45 C.F.R. § 164.312(c)
15. 45 C.F.R. § 164.312(e)(2)(i).

***Jonathan P. Tomes** (jon@tomesdvorak.com) is a partner at Tomes & Dvorak and president of EMR Legal, a HIPAA consulting firm, in Overland Park, KS.*

Article citation:
Tomes, Jonathan P. "Spoliation of Medical Evidence." *Journal of AHIMA* 76, no.9 (October 2005): 68-72.