

Effective and Compliant Records Management Policies for Health Care Providers and Suppliers

Legal and Practical Issues Providers Should Consider When Reviewing Current Practices

Karen S. Lovitch and Heather L. Westphal

Records management has taken on added significance for companies nationwide since the Enron/Arthur Andersen scandal and the enactment of the Sarbanes-Oxley Act in 2002. In light of these recent developments, all corporations should examine their records management policies and practices to evaluate compliance with federal, state, and industry standards. This process is especially important for health care providers and suppliers (referred to collectively as "providers" herein) in light of the hostile litigation and enforcement environment in which they must operate.

Discovery requests in malpractice and other legal actions as well as subpoenas in government investigations routinely request a lengthy laundry list of patient and other facility documentation that can be used against the provider. Although the first priority must be to retain records consistent with good business practices and applicable law, a health care provider also must consider what records it is *not* required to keep for a specified period of time and determine how long it should maintain them. A provider cannot be required to produce records that it has lawfully destroyed.

This article will give health care providers an overview of the current legal and practical issues they should consider when reviewing their current records management policies and practices. It will discuss the basic elements of a records management policy, the advantages of effective and compliant policies, and the particular legal and other requirements for retaining various types of records. It will conclude with recommendations for effective implementation.

Records Management Policy Basics

Records management policies establish protocols for handling the various types of records

that a company produces and receives from outside sources.¹ Every company should tailor its policies to its specific needs, but some generalizations are possible. Records management policies usually cover issues such as responsibility for oversight of the policy's implementation, the exact definition of a record, the types of records that a company should preserve permanently, treatment of certain types of records such as duplicate copies of the same record and electronic records, and circumstances in which the company should never destroy records, such as when litigation or an investigation is pending or reasonably anticipated.²

Records management policies are not complete without a retention schedule, which provides a detailed inventory of every type of record that the company produces or keeps on file.³ The schedule usually is divided into categories of records, such as accounting or finance, human resources, and sales or marketing, and it sets forth a minimum timeframe for retention of each possible type of record within those categories.⁴

For instance, a health care provider's retention schedule likely would include a category for records related to billing and reimbursement for services. Within that category, the provider would establish separate retention periods for each type of relevant document, such as cost reports and claims for payment.

Advantages of Effective and Compliance Records Management Policies

Most, if not all, companies understand that retaining and periodically destroying certain types of records makes good business sense for a variety of reasons. In the context of the *Arthur Andersen* case, companies learned the importance of preserving documents upon discovering possible wrongdoing that would lead to a government investigation or litigation. The advan-

tages of effective and compliant records management policies, however, extend far beyond this scenario.

Compliance with Legal Requirements/Guidance from the Office of Inspector General

Given the scrutiny paid to the operations of health care providers and the specific record-keeping requirements applicable to them, they must not only develop records management policies but also implement those policies effectively to ensure legal compliance.⁵ The Department of Health and Human Services' Office of the Inspector General (OIG) has issued compliance program guidance for various sections of the health care industry. Each guidance recommends that the provider develop and implement a record retention policy and maintain records according to the needs that are specific to that particular industry.

For example, DMEPOS suppliers "should ensure that records are maintained for the length of time required by federal and state law and private payors, or by the DMEPOS supplier's record retention policies, whichever is longer."⁶ Similarly, the OIG guidance for hospitals recommends that hospitals retain all records and documentation required for participation in federal health care programs, such as clinical and medical records and claims documentation, as well as all records necessary to protect the integrity, and document the effectiveness of, the hospital's compliance program.⁷

Implementation of the OIG's compliance program guidances is voluntary, but heeding the OIG's recommendations regarding record retention is nevertheless prudent because sound records management policies will assist health care providers in complying with the countless record retention requirements imposed by law.

Although many of these laws are applicable to all companies, health care providers have an increased burden in light of the additional layer of legal requirements with which they must comply. For instance, as virtually every provider knows, the retention of clinical records is regulated at the state and federal levels. In particular, federal regulations require hospitals participating in the federal health care programs to retain medical records for a period of at least five years.⁸

Additionally, the Medicare program requires all providers to retain clinical records for the period of time required by state law, for five years from the date of discharge if state law does not specify a timeframe, or, in the case of a minor, for three years after the patient reaches legal age under state law.⁹ The deference to state law is important to note because most, if not all, states have specific requirements for the retention of medical records,¹⁰ and more and more states are enacting requirements for specific types of medical records, such as x-rays and laboratory test results.¹¹

Noncompliance with these requirements can have vast consequences, such as loss of state licensure or federal certification or, at the very least, monetary or other

sanctions imposed in the context of a state or federal survey. Moreover, as discussed in the following section, if noncompliance is discovered in the context of a third party subpoena or a discovery request in pending litigation, it can have even more serious ramifications.

Protection from Charges of Obstruction of Justice or Improper Destruction of Records in the Context of Litigation

Effectively designed and implemented records management policies can prove invaluable in civil and criminal litigation.¹² Such policies can provide protection from civil liability for improper destruction of records and, perhaps more importantly, charges of criminal obstruction of justice under state or federal law.¹³

This protection is implemented through the policy's stop function, which instructs employees how and when to suspend routine destruction of records pursuant to the policy.¹⁴ The stop function plays an important part in litigation because a company may be subject to sanctions for destroying documents if it "knows or reasonably should know that the evidence might be relevant to a possible action."¹⁵ The legal term for this concept is "spoliation" of evidence. Spoliation can have negative consequences even if the destruction was unintentional.¹⁶

A finding of spoliation can adversely affect a party's position in litigation. The court has wide discretion in imposing sanctions and can even dismiss the case or enter a default judgment.¹⁷ The court also may instruct the jury that it can infer the missing records were harmful to the party unable to produce them.¹⁸

A defending party unable to produce records integral to the other party's position also could be required to demonstrate its innocence even before the complaining party presents its case. For instance, the Florida Supreme Court held in a medical malpractice action that the burden of proof must shift to the hospital if it negligently failed to produce essential medical records and that failure hindered the plaintiff's case.¹⁹ Finally, the court may sanction a party that suppresses or destroys evidence by precluding that party from introducing evidence critical to its case.²⁰

Courts also have the discretion to impose monetary sanctions upon litigants who destroy documents that are relevant to a pending or potential case or that reasonably could lead to the discovery of admissible evidence.²¹ Monetary sanctions may include fines or reasonable attorneys' fees and expenses and can be very costly.²² For example, a federal district court in New Jersey imposed a \$1 million sanction against a company for improperly destroying electronic data that impaired the plaintiff's ability to establish its claims.²³

Some states have recognized spoliation as a tort that, if proven, can result in the imposition of monetary damages separate and apart from any monetary sanctions imposed by the court.²⁴ In Louisiana, for example, a litigant may bring a separate state law claim for intentional spoliation based on the "intentional destruction of evidence carried out for the purpose of depriving an opposing party of its use."²⁵

A handful of states even recognize a tort for or at least allow a separate claim based upon negligent spoliation.²⁶ Even so, most courts that have considered this issue have declined to recognize such a tort given the existence of other remedies and the cost of additional litigation that may result from recognition of the tort.²⁷

Finally, as demonstrated by the *Arthur Andersen* case, criminal obstruction of justice charges can result in harsh criminal penalties. Most criminal obstruction of justice statutes provide for hefty fines as well as imprisonment, and prosecutors often pursue charges against the company as well as the individuals involved in the destruction. For example, the federal government prosecuted Arthur Andersen for its destruction of documents related to a Securities Exchange Commission investigation and later sentenced the company to the maximum penalty of \$500,000 and five years of probation.²⁸ A former Arthur Andersen employee, David Duncan, also was pursued by the federal government²⁹ and ultimately pled guilty to criminal charges.³⁰

Defense Against "Fishing Expeditions"

Nearly all companies are aware by now that the unlawful destruction of documents can cause enormous damage to a company's finances as well as to its reputation, but few focus on the fact that the *lawful* routine destruction of documents pursuant to properly implemented records management policies often can benefit a company. Nearly all health care providers are familiar with the "fishing expeditions" conducted by plaintiffs' lawyers and government investigators. For instance, in a quality of care investigation, the government may seek a host of patient-related records, billing records, audit and survey documentation, provider agreements, and a long list of documents maintained by management (such as shift-to-shift communication books, quality assurance records, and staffing logs).

Notably, in many instances, the documentation requested by litigants or by government investigators is not required by law to be maintained for a specified period of time. Examples include certified nurse aide care logs, facility policies and procedure manuals, and time and attendance records.³¹

If the provider lawfully destroys such documents when litigation is not threatened or expected,³² the chances that such a fishing expedition will result in success are greatly reduced because a provider cannot be required to produce documents that it has lawfully destroyed. For example, a health care provider may decide to routinely destroy clinical documents that are not part of the patient's medical record, such as nurse aide assignment sheets or shower schedules maintained by hospitals and long-term care facilities, in the absence of a state or federal statute or regulation requiring their retention. If later sought in a subpoena or discovery request, these documents, which often contain damaging information, cannot (and are not required to) be produced.

Administrative Convenience and Cost Savings

Yet another benefit of effective and compliant records management policies is that they save the company time and money. Keeping every document in storage without a legal or business justification for doing so is neither practical nor efficient.³³ To provide a full response to any subpoena or discovery request, the company must search through *all* potentially relevant paper or electronic records, which could result in enormous administrative costs for the company.

If documents are routinely, lawfully destroyed, an employee's search for documents can be expedited, whether responding to requests for documents received in connection with a subpoena or discovery request or just carrying out day-to-day duties. In addition, the lawful, routine destruction of documents can result in a cost savings for companies if less storage space is required for hard copy and electronic documents.

Creation of Effective and Compliance Records Management Policies

Effective records management policies come in many different packages, but every company's policies should reflect its specific needs and legitimate business purposes.³⁴ Legal compliance and administrative convenience, rather than a desire to purge potentially damaging documents from the company's files, should motivate the adoption of appropriate records management policies.³⁵

Every health care provider planning to create new policies or to reevaluate its existing policies and practices should begin by consulting a knowledgeable health care attorney because compliant policies must be premised upon an understanding of legal requirements as well as industry standards. Providers operating in more than one jurisdiction must consider the laws of all applicable states.

Step One: Establish a Comprehensive List of Records

The process should begin with an evaluation of the types of records retained by the company. All department heads should be surveyed to make this determination, and personnel at the local and corporate levels likely should be included as well. The survey should cover issues such as the types of records generated by the company and those received from inside and outside sources.

Employees also should provide information regarding current knowledge of applicable state and federal laws or regulations governing records management practices as well as the formal and informal policies and procedures they follow on a daily basis. Based upon the results of this survey and the company's current records management policies, if any, the company should, with the assistance of legal counsel, create a comprehensive list of records.

Step Two: Draft the Policies

As stated above, the purpose of records management policies is to establish protocols for the organization,

storage, and destruction of various paper and electronic records that a company produces and receives from outside sources. Although every company's policies differ according to individual needs, all should consider certain key issues.

Defining a "Record"

As mentioned above, the term "record" must be defined so that employees may understand how to execute the company's records management policies. Generally, a "record" includes hard copy and electronic documents, incoming as well as outgoing information, and all documents regardless of their location, including those kept at an employee's home. The definition should clearly encompass records an employee may consider personal, such as email and calendars detailing business activities.

The inclusion of electronic records presents challenges for all companies, including health care providers. According to at least one account, 93 percent of all business documents are created electronically and only 30 percent are ever printed to paper.³⁶ Nearly all companies use back-up tapes to store emails, word processing files, spreadsheets, and other electronic information.³⁷

Unfortunately, files stored on back-up tapes often are kept much longer than necessary and therefore can needlessly become the subject of discovery requests or subpoenas. Considering the voluminous amount of information on even just one tape, production of these tapes can result in great expense to the company and possibly the production of damaging information that otherwise may have been destroyed.

To avoid this situation, records management policies should require the routine destruction of all electronically stored copies and versions of the documents consistent with the destruction of hard copy documents. The destruction of electronic records in every storage location must be ensured.³⁸ In addition, such destruction must be permanent so that the documents cannot be recreated or otherwise retrieved at a later date.³⁹

Suspension of Routine Destruction

The circumstances in which routine destruction must cease should be clearly articulated in every company's records management policies. Employees should receive instructions regarding how to proceed upon receiving notification of the suspension of routine destruction and upon gaining knowledge of a pending or threatened proceeding because one employee's knowledge may be imputed to the entire company.

Appropriate suspension of routine destruction will not only provide protection from civil and criminal liabilities and other consequences of spoliation but also may help a health care provider exonerate itself in litigation or in an investigation by ensuring retention of favorable records or evidence.⁴⁰ For example, a provider may easily respond to allegations of inadequate quality of care allegations in a government investigation by provid-

ing documentation from the patient's properly retained clinical record supporting the provision of appropriate care provided to the patient(s) at issue. If such documents had been scheduled for routine destruction, and such destruction was not suspended upon learning of the litigation, then the provider may not have had the clinical records on file necessary to defend itself.

Consistency with HIPAA

Health care providers must consider the intersection between records management policies and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations. All providers are acutely aware of HIPAA's rules regarding the use and disclosure of a patient's protected health information. When evaluating general records management policies, providers should be mindful of the promises made to patients regarding the availability and destruction of information in their notices of privacy practices provided pursuant to HIPAA.

For instance, if a provider agrees to maintain the information for no longer than is necessary to fulfill the purposes for which it is collected, the provider must ensure destruction consistent with its general records management policies and with state and federal law.⁴¹ In addition, HIPAA requires providers to maintain documentation of compliance with its requirements for a period of at least six years.⁴²

Document Storage Methods

A records management policy likely cannot succeed unless it is premised on a uniform, centralized system of storage.⁴³ This issue is especially significant for health care providers because they must store a wide variety of patient care, administrative, and other records. In the health care industry, the focus is understandably on the provision of quality patient care rather than on mundane administrative concerns like creating effective storage systems.

As a result, many health care providers may have inadequate storage systems in need of reevaluation. Health care providers should reconsider their methods for storing electronic records (single versus multiple hard drives, individual computers versus CD-rom/discs or both), the use of centralized filing areas or storage spaces, and the possible need for off-site storage.⁴⁴

Step Three: Develop a Retention Schedule

Every company's records management policies should be accompanied by a retention schedule consisting of a retention period for each type of document on the company's comprehensive list of records. The company should work closely with knowledgeable health care counsel to determine these retention periods.

Legally Mandated Retention Periods

As stated above, statutes and regulations dictate the retention periods for many documents. A health care

provider must cast a very wide net to determine the relevant state and federal statutes and regulations because those applicable to all businesses apply, as do those specifically governing health care providers or even specific provider types, such as nursing homes, hospitals, or clinical laboratories.

Federal law sets a number of retention periods that are relevant to health care providers. For instance, the statutes and regulations enforced by the various agencies within the Department of Labor speak to a company's retention of a variety of documents, including pre-employment tests, employment applications, job opening advertisements, and employee injury reports.

Nearly all employers must comply with these statutes, which include the Fair Labor Standards Act⁴⁵ and the Occupational Safety and Health Act.⁴⁶ An example of a more specific document retention requirement is the previously mentioned federal regulation requiring hospitals certified to participate in Medicare, Medicaid, or other federal health care programs to maintain medical records for a certain period of time.⁴⁷

Many record retention periods are established by state law as well. These requirements are particularly important because many federal statutes and regulations defer to state law. States regulate the retention of a variety of general business and other records, including, of course, patient records. Providers should note that the requirements for patient records may differ if a patient is a minor, is affected by mental illness or mental retardation, has certain designated medical conditions (such as substance abuse or AIDS), or is deceased.

Determining applicable legal obligations in this regard is complicated by the fact that retention requirements often appear in agency manuals and other forms of agency guidance, particularly at the state level. For instance, state Medicaid program manuals and issuances often announce record retention requirements, and those requirements occasionally conflict with the standards set by the Medicare program.

Providers should work with knowledgeable health care counsel to determine whether to exceed legal requirements based on industry standards and other considerations. Business needs, standards set by accreditation agencies or industry trade associations, or applicable audit or survey periods may lead a provider to keep documents for a longer period of time.

Providers also must consider the relevant statutes of limitation, which often allow a litigant to file suit long after retention periods have expired. For instance, the federal False Claims Act allows a whistleblower to bring an action up to 10 years after the alleged violation occurred.⁴⁸ Moreover, most states have established statutes of limitation for certain types of legal actions, and they can vary widely.

In Virginia, for example, the statute of limitations for a personal injury action is two years, but this period is extended in a medical malpractice action in certain cir-

cumstances.⁴⁹ Virginia also sets a two-year limitation period for wrongful death actions, a five-year period for an action based on a written contract, and a three-year period for an oral contract action.⁵⁰ Health care providers unfortunately must assume that certain records—particularly those related to patient care—may become the subject of a lawsuit or government investigation at some point in time.

Providers, therefore, must work with legal counsel in deciding whether to retain documents beyond the legally required retention periods consistent with statutes of limitation. Such decisions are very complex given that predicting whether certain documents will help or hurt in litigation is extremely difficult.

Retention Periods Set by Contract

Health care providers contract with a variety of entities, such as private third party payors, state and federal governments, and vendors. Providers should consider whether these and other contracts require retention of relevant records for a specified period of time.⁵¹ A health care provider should actively negotiate record retention requirements in every contract to ensure consistency with its own records management policies.

Retention Periods Not Governed by Law or Contract

To determine retention periods that are not dictated by law or contract, providers should begin with an evaluation of the document's purpose. For each category or subcategory of documents, a provider should consider who creates the document, who uses the document, and for what purpose. In other words, a document should be retained consistent with business needs.

Many of the same considerations bearing on the decision whether to exceed retention requirements mandated by law (if any) apply here as well. Providers should consider the applicable statutes of limitation and standards set by accreditation agencies and industry trade associations.

For example, according to the standards of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), the retention period for medical record information maintained by long-term care providers should be "determined by law and regulation and by its use for resident care, legal, research, or educational purposes."⁵² The intent accompanying this standard provides that records should be retained for "the period of time required by state law, or five years from the discharge date when there is no requirement in state law."⁵³ Providers also may seek guidance from the American Health Information Management Association (AHIMA), which has published recommendations for health care providers on the retention of patient health information.⁵⁴

Finally, applicable audit, survey, or accreditation periods may affect a health care provider's decisions on retention of records. For example, a provider may decide

to retain a document responsive to a regulatory requirement, even though there is not specific retention period for that particular document, long enough to ensure that it is available at the time of the next survey.

Step Four: Implement Effectively

Once crafted, a records management policy is of little use unless the company actually implements the policy consistent with its terms at every level. Having a corporate policy that is ignored or not enforced at the facility or the department level is potentially as damaging as no policy at all.

Every company should designate a records management officer who is responsible for administering the policies in a centralized, cohesive fashion. He or she must work with a variety of other people, including management, information services representatives, and legal counsel, to ensure proper implementation on an ongoing basis. The records management officer also serves as a resource for employees who have questions or concerns about records management.

Effective implementation depends upon the awareness and understanding of all employees. The records management officer must ensure that all employees receive training with regard to the policies and then follow up this training with periodic reminders and refresher sessions, which are most effective when no litigation or investigation is threatened or pending. Employees (particularly department heads and managers) should be reminded that failure to comply with the policies will be addressed in annual performance evaluations and can have legal ramifications not only for the company but also for the individual employee.

Conclusion

Although nearly every company gives lip service to appropriate document destruction and retention, few actually take the action necessary to implement effective and compliant records management policies. In the current operating environment, which is characterized by frequent government investigations and litigation and ongoing compliance and corporate responsibility concerns, this issue—which can and has destroyed an entire company—must take center stage for all companies. The resources spent on developing and properly implementing records management policies will benefit the company in countless ways and complement its existing compliance, risk management, and cost containment efforts.

References

1. Daniel B. Trinkle & Breton Leone-Quick, "The Importance of Records Management for Biotech and Life Sciences Companies," *J. Biolaw & Bus.*, Vol. 6, No. 3, 2003, at 27; Michael E. Arruda, Margaret R. Prinzing, & Shruti A. Rana, "Documents? What Documents?," *Business Law Today*, Jan./Feb. 2003, at 23.
2. See Trinkle & Leone-Quick, *supra* note 1, at 27.
3. *Id.*
4. See *Id.*

5. See Trinkle & Leone-Quick, *supra* note 1, at 28 (discussing the importance of effective implementation for biotech companies).
6. Publication of the OIG *Compliance Program Guidance for the Durable Medical Equipment, Prosthetics, Orthotics and Supply Industry*, 64 *Federal Register* 36368, 36380 (July 6, 1999).
7. Publication of the OIG *Compliance Program Guidance for Hospitals*, 63 *Federal Register* 8987, 8993 (Feb. 23, 1998).
8. 42 C.F.R. § 482.24(b)(1) (2003).
9. Medicare Claims Processing Manual, CMS Pub. 100-04, Ch. 1, § 110.3.
10. See, e.g., 22 Tex. Admin. Code § 165.1(b) (2004) (requiring physicians to retain medical records for a period of seven years following the most recent treatment of the patient, or if a patient was under age eighteen when last treated, until the patient reaches age 21 or seven years from the last date of treatment, whichever is longer).
11. See Cherylyn Murer, Michael Murer & Lyndean Lenhoff Brick, *The Complete Guide To Healthcare Records Management* at 235 (2000). For example, the State of New Jersey requires long-term care facilities to retain X-ray films or reproductions of them for a period of five years. N.J. Admin. Code tit. 8, § 8:39-35.2(k). Similarly, New Mexico law requires hospitals providing laboratory services to maintain laboratory test results and records for a period of four years after the test or, for patients who are minors, for one year beyond the age of majority. N.M. Admin. Code tit. 7, § 7.2.30(D) (2004).
12. Trinkle & Leone-Quick, *supra* note 1, at 28.
13. See, e.g., 18 U.S.C. § 1503 (2004) (preventing obstruction of justice as a general matter); 18 U.S.C. § 1505 (forbidding destruction of documents relevant to a pending agency or congressional proceeding); 18 U.S.C. § 1512 (prohibiting coercion or attempts to coerce or mislead another person to withhold, alter, or destroy documents in connection with an official proceeding); D.C. Code Ann. § 22-723 (2004) (establishing that a person who "alters, destroys, mutilates, conceals, or removes a record, document, or other object, with intent to impair its integrity or its availability for use in the official proceeding" is guilty of obstruction of justice); Neb. Rev. Stat. Ann. § 28-102 (2004) (classifying the destruction of documents in connection with a pending or anticipated official proceeding as a felony). In response to the *Arthur Andersen* case, Congress passed the Sarbanes-Oxley Act of 2002 (SBO Act), which resulted in the enactment of two new obstruction of justice statutes specifically targeting improper destruction or alteration of documents or evidence. See 18 U.S.C. § 1519, 1520. The SBO Act also amended 42 U.S.C. § 1512 to ensure that the statute covers the person who actually destroys the documents, in addition to the person who persuades another to do so.
14. See Trinkle & Leone-Quick, *supra* note 1, at 29.
15. See *id.* (citing *Kippenham v. Chaulk Servs., Inc.*, 428 Mass. 124 (1998)).
16. See Trinkle & Leone-Quick, *supra* note 1, at 29 (citing *Kelley v. United Airlines, Inc.*, 176 F.R.D. 422 (D. Mass.1997)).
17. See *United States v. Taber Extrusions*, 2001 WL 1941318 (E.D. Ark. 2001) (citing *Sanctions, The Federal Law of Litigation Abuse—Inherent Power: Bad Faith Litigation Abuse*, § 28(A), at 450 (3d ed., Gregory P. Joseph, ed., 2000)).
18. See *Cedars-Sinai Medical Ctr. v. Super. Ct. of Los Angeles*, 954 P.2d 511, 517 (Cal. 1998).
19. *Public Health Trust of Dade County v. Valcin*, 507 So. 2d 596 (Fla. 1987). There, the plaintiffs claimed that the hospital's inability to produce a surgical report, which was required by law to be maintained, adversely affected their case because the lack of report impaired the ability of plaintiffs' expert to render a conclusive opinion. *Id.* at 597. The court found that, if the plaintiff can demonstrate the absence of records "hinders his ability to establish a prima facie case," a rebuttable presumption shifting the burden of proof applies to "equalize the parties' respective positions in regard to the evidence and to allow the plaintiff to proceed." *Id.* at 599-600.

20. See Trinkle & Leone-Quick, *supra* note 1 at 29 (citing United States Filter Corp. v. Ionics, Inc. 128 F. Supp.2d 56 (D. Mass. 2001)).
21. See *United States v. Taber Extrusions*, 2001 WL 1941318 (E.D. Ark. 2001) (citation omitted).
22. See *id.*
23. See Trinkle & Leone-Quick, *supra* note 1, at 29 (citing *In re Prudential Ins. Co. Sales Practices Litig.*, 169 F.R.D. 598, 617 (D.N.J. 1997)).
24. Kenneth B. Abel & Benjamin J. Rubin, "Advising Business Clients on Document Retention Policies," *MD. B. J.*, Jan./Feb. 2004, at 30, 35.
25. *Burge v. St. Tammany Parish*, 336 F.3d 363, 374 (5th Cir. 2003) (citing *Pham v. Contico Int'l, Inc.*, 759 So. 2d 880 (La.App. 5 Cir. 2000)); see also Abel & Rubin at 35.
26. See, e.g., *Hannah v. Heeter*, 584 S.E.2d 560, 566-568 (W.Va. 2003) (recognizing spoliation as a stand-alone tort where the spoliation results from the negligence of a third party who had a special duty to preserve the evidence, but declining to recognize such as a tort with respect to a party to the litigation).
27. *Id.* at 566 n. 8.
28. Brenda Sapino Jeffreys, *Andersen Gets Maximum Sentence for Obstruction of Justice*, *Texas Lawyer*, Oct. 17, 2002, available at <http://www.law.com/jsp/article.jsp?id=1032128761960>.
29. Tom Fowler, *Duncan Aide Tearfully Tells of Boss's Firing*, *Houston Chronicle*, June 15, 2002, <http://www.chron.com/cs/CDA/story.htm/special/andersen/1434968>.
30. *Id.*
31. This statement is a broad generalization regarding state document retention requirements. Individual state laws requiring retention of documents could exist, and, as suggested in this article, every provider should consult knowledgeable health care counsel for advice on such issues.
32. If retention is not legally required, and a provider decides not to keep a certain type of document in the normal course of business, a subpoena or discovery request cannot and should not be read as imposing such a requirement.
33. Trinkle & Leone-Quick, *supra* note 1, at 29.
34. See *Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988) (assessing the reasonableness of a company's document retention policy). In *Lewy*, the court established a three-part test for evaluating a company's policy: (1) whether the retention period was reasonable, considering the document in question; (2) whether lawsuits have been filed based on similar complaints; and (3) whether the policy was adopted for legitimate business purposes or in bad faith. *Id.*
35. Trinkle & Leone-Quick, *supra* note 1, at 29; see also *Lewy*, 836 F.2d at 1112.
36. Michele C.S. Lange, "Sarbanes-Oxley Has Major Impact on Electronic Evidence," *Nat'l L. J.*, Jan. 2, 2003.
37. Trinkle & Leone-Quick, *supra* note 1, at 29.
38. Trinkle & Leone-Quick, *supra* note 1, at 30.
39. *Id.*
40. *Id.*
41. Arruda, et al., *supra* note 1, at 25.
42. 45 C.F.R. § 164.530.
43. See Trinkle & Leone-Quick, *supra* note 1, at 30.
44. *Id.*
45. 29 U.S.C. § 201 *et seq.*
46. 29 U.S.C. § 651 *et seq.*
47. 42 C.F.R. § 482.24(b)(1).
48. 31 U.S.C. § 3731(b)(1)-(2).
49. Va. Code Ann. § 8.01-243 (2004). The statute of limitations is lengthened for a period of one year from the date that a person discovers or reasonably should have discovered "a foreign object having no therapeutic or diagnostic effect being left in [his or her] body." § 8.01-243C. 1. In addition, if "fraud, concealment or intentional misrepresentation prevented discovery of the injury" within the two-year period, the action may be brought within one year from the date that the injury was discovered or reasonably should have been discovered. § 8.01-243C.2.
50. Va. Code Ann. § 8.01-244 (wrongful death); Va. Code Ann. § 8.01-246(2) (written contract); Va. Code Ann. § 8.01-246(4) (oral contract).
51. Arruda, et al., *supra* note 1, at 25.
52. Joint Commission on Accreditation of Healthcare Organizations, *Comprehensive Manual for Long-Term Care, 2003-2004*, at IM-11.
53. *Id.*
54. Donna M. Fletcher & Harry B. Rhodes, *Practice Brief: Retention of Health Information* (Updated), June 2002, available at http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bokl_012545.html. Generally, AHIMA recommends that, in the absence of state specific requirements, providers should retain health information for at least the period specified by applicable state statutes of limitation or for "a sufficient length of time to prove compliance with laws and regulations." *Id.* AHIMA warns, however, that a longer retention period is "prudent" because the statute of limitations may not begin to run until a potential plaintiff knows or reasonably should know of the claim and because the False Claims Act has a limitation period of 10 years. *Id.* **JHCC**