The Case Is Closed.

By Shannon Spangler, Anne Kershaw and Julie Richer

Where Are Your Documents?

30-SECOND SUMMARY
Corporate documents placed in the care of third parties must be accounted for. Documents neither destroyed nor returned when a case is closed represent ongoing exposure. Three steps can help to ensure that the final case closing will be routine and easily managed: 1) Set expectations with outside counsel with respect to case closing. 2) Put a tracking process in place during litigation before entrusting documents and data to third parties. 3) Make no final payments until satisfied that all documents have been returned or destroyed.

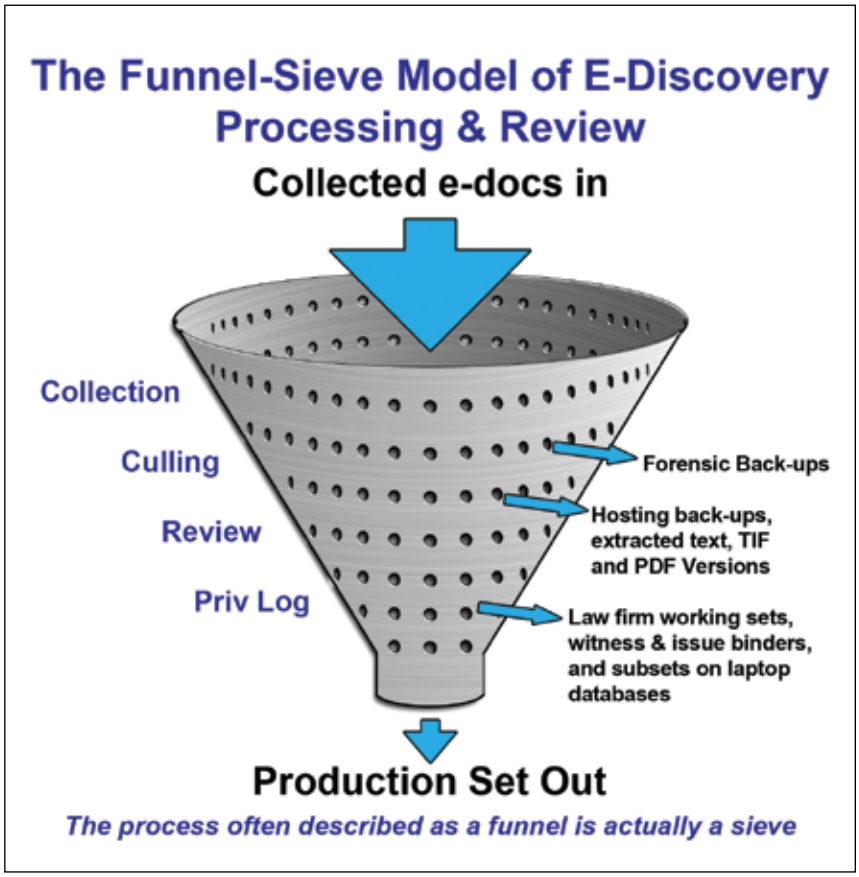
After years of protracted wrangling, your case has settled. But don't pop the corks on those champagne bottles just yet. Do you know where all the copies of your documents are — the ones that were turned over to outside counsel, consultants, forensic experts, processing vendors, database hosting providers and opposing counsel? Chances are that at least some of those copies are far less protected than if they were sitting behind the corporate firewall — and the copies being held by law firms may be at the greatest risk. For example, in 2009, the FBI issued a warning to law firms that they could be the focus of hacker attacks, and some experts think it would only take a C-grade hacker to penetrate a law firm's security infrastructure.

In most companies, law departments own the relationships with outside law firms, ediscovery processing vendors, experts, consultants and hosting vendors. Thus, law departments are normally charged with ensuring that company documents handed over to those third parties are secure while outside the corporation's firewalls, and are returned or destroyed when the third parties no longer need them.

What steps should you take today to assert control over company documents and data placed in the care of third parties in connection with legal matters? How do you enlist your law firms as full partners in the case closing process? This article offers some simple and workable suggestions on closing case files.

Every copy of every document multiplies the risk of its misuse. All copies of the corporation's documents that are unaccounted for, and neither destroyed nor returned, represent ongoing exposure. For example:

- *Future litigation or investigations:* Copies of data that the corporation had every right to dispose of after the case closed can be swept up in discovery in subsequent litigation or governmental investigations, either by subpoenas or document requests issued to the corporation or any third parties who hold your data. The costs of repeatedly reviewing data that could have been deleted can be quite significant.
- *Data breach liability:* Copies may contain private information pertaining to clients, patients, suppliers, employees and other stakeholders. The corporation will typically remain liable for breaches of its data content while in the hands of third parties with whom it contracted, especially if the corporation is in the health industry or financial sector. The penalties can be significant, particularly if the data originated in the EU or other jurisdictions with stringent data privacy laws.
- *Trade secret disclosure:* Discovery documents can contain extremely sensitive information, including data regarding patents, production processes, formulae, suppliers, employees, security measures, product plans and so forth; the list is endless. Your organization may do a splendid job of protecting information behind its firewalls, but the same level of care and security may be sorely lacking for data held by third parties. This can lead to inadvertent disclosure caused by carelessness, such as a vendor's failure to completely wipe the company's data from servers before disposing of them, or disclosure

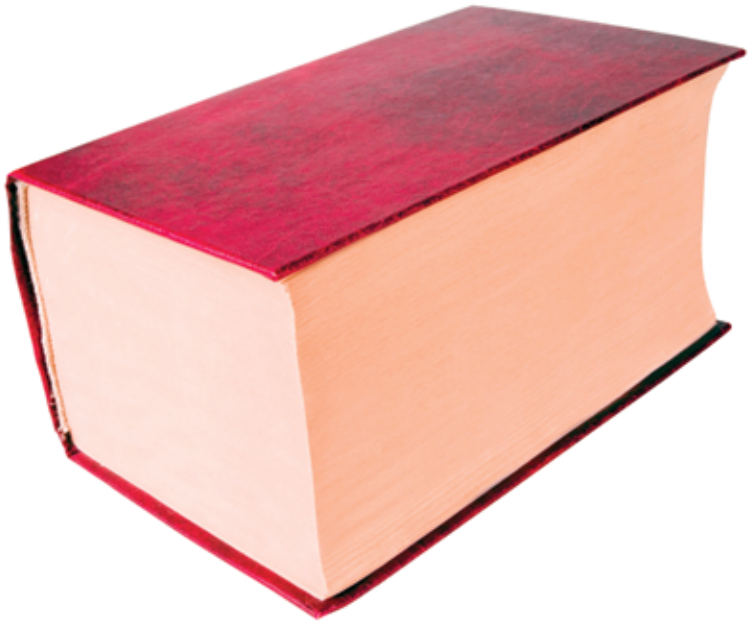


Shannon Spangler served as associate general counsel, Altria Client Services, from 2005 to 2012, after many years with Shook, Hardy & Bacon as partner and office managing partner. Spangler is currently in Columbia University's Information and Knowledge Strategy M.S. program. *shannon@slspanglerpc.com*

Anne Kershaw is founder of A.Kershaw Attorneys & Consultants, faculty member in Columbia University's Executive Master of Science in Information and Knowledge Strategy program, and advisory board member of the Georgetown University Law Center's Advanced Ediscovery Institute. *anne.kershaw@akershaw.com*

Julie Richer is legal technology program manager at American Electric Power, where she is responsible for matter discovery as well as managing the legal operations team. Prior to transferring to legal in 2008, she spent 10 years in AEP's IT Department. *jmricher@aep.com*

What if authors were paid by the word?



For one thing, most books would look like this.

There's a good reason authors are paid for the quality of what they say, not for how many words they use.

That's why Tucker Ellis rewards its attorneys for delivering what clients value – exceptional service, professional excellence, teamwork, and integrity – not for the number of hours they bill.

Many firms talk about alternative fees. For us, getting away from "billable hours" is the foundation of who we are. More than 60% of our fees are earned through arrangements other than the billable hour.

The future of the legal industry is here.

Tucker Ellis | LLP

CLEVELAND COLUMBUS DENVER LOS ANGELES SAN FRANCISCO | tuckerellis.com

Joe Morford, Managing Partner joseph.morford@tuckerellis.com

as a result of industrial or foreign government espionage efforts.

- *Data mining:* Data analytics, as applied to "big data," can yield insights and relationships that are not obvious from an examination of individual documents. Selling "big data" is big business. As long as large collections of a company's data are unaccounted for, those collections could be part of a competitor's data mining operation. Litigation presents a unique opportunity to collect and aggregate data that would typically not be analyzed together.
- *Orphaned or unattended data sets:* Even if your law firm is exceptional in terms of data security, what happens if it goes out of business? Remember Howrey LLP, Dewey & LeBouef, or Broebeck Phleger & Harrison? While there's nothing to suggest that data held by those firms was put at any additional risk as a result of the breakups, should the corporation take that chance if it can avoid it by the simple expedient of getting its own data back? Even short of a firm-wide breakup, what happens to your documents when the paralegal or associate who has been handling your documents moves to another law firm, leaving your documents under the management of someone in whom you may not have complete confidence?

Copies of the corporation's data can exist in many forms, in many places. The purpose of the case closing process is to destroy or recover all copies of the corporation's documents and data disseminated in connection with litigation or other legal matter. But where are they? Consider the following:

- *Has your outside counsel neglected case closing procedures for previously closed matters?* If you and your outside counsel have not implemented strong case closing processes for matters that came to an end some time ago, you may need to ask your firms what they have and where it is, and insist on a housecleaning process.
- *Going forward, address case closing procedures throughout all phases of litigation.* It simply may be too late to effectively implement case closing procedures after all of the case activity has taken place. At a minimum, both you and your law firm will face a significant amount of unplanned work, which will get between you and that bottle of celebratory champagne. Instead, if you take three series of steps — at the beginning, in the middle and at the end — the final case closing will be routine and easily managed.
- *In the beginning, set expectations with outside counsel.* In your engagement letter with outside counsel inclue requirements that are critical to case closing (see box above). Consider sharing with your firms the case-closing checklist you will use at the end of the matter to check and evaluate the firm's compliance with the engagement letter (see sidebar on page 62).
- *During the litigation, follow appropriate safeguards and protocols when handing over company documents and data, whether they are going to your law firm or another third party.* Put in place some sort of tracking process, such as a simple inventory, before

Case-closing clause for outside counsel retention agreement

Case-Closing Process. **Company documents and data ("Documents") provided to outside counsel ("Counsel") for purposes of discovery and investigation must be destroyed or returned to Company at the conclusion of the matter, as directed by Company. Counsel shall provide a closing report to Company that memorializes the disposition, or return decisions made with respect to Company Documents within 30 days of the case being closed, which is defined as meaning that the opposing party is precluded from further action in the case, either because the time for all appeals has run out or because a binding settlement agreement has been entered. If the data is disposed of by counsel, appropriate steps must be taken to ensure the protection of confidential and private information. Legal files pertaining to Company matters are considered to be the property of Counsel and should be maintained in accordance with the law firm's document and data retention and disposition policies. Company documents that have been incorporated into pleadings, motions or other filings are considered to be part of the legal file. The payment of final invoices for any matter will be suspended pending notice from counsel that appropriate file closure procedures have been completed as evidenced by a completed Certificate of Destruction and Non-Breach as shown in Attachment X hereto.**

Data Breach Indemnification, Notification and Certification. **Counsel agrees to indemnify and hold Company harmless from any and all costs, liabilities or other expenses arising from a data breach of Company Documents while in the possession, custody or control of Counsel. Counsel agrees to provide immediate notice to Corporation if there are any known or suspected data breaches of the documents provided by Corporation to Counsel. At the conclusion of the case, Counsel agrees to certify the return or destruction of all corporation documents as described above, and to certify as to whether there has been any known or suspected data breach pertaining to those documents.**

PEOPLE WHO MAKE GREAT COMPANIES WORK

For nearly 30 years, specialists at CDW have provided technology solutions to thousands of organizations around the globe. Enterprise Solutions Manager Nathan Coutinho and his team at CDW work with clients in a broad range of industries, helping them maximize their technology investments. Experienced, innovative, and deeply knowledgeable about leading technologies, Nathan and the CDW team are masters at solving their clients' most pressing challenges. "Operational efficiency is a driver of our clients' success," says Nathan. "We work hard to understand each client's unique challenges and give them a competitive edge." Perkins Coie is proud to provide a wide range of legal services to CDW.

Perkins Coie: Legal Counsel to Great Companies like CDW.

ANCHORAGE · BEIJING · BELLEVUE · BOISE · CHICAGO · DALLAS · DENVER
LOS ANGELES · MADISON · NEW YORK · PALO ALTO · PHOENIX · PORTLAND
SAN DIEGO · SAN FRANCISCO · SEATTLE · SHANGHAI · TAIPEI · WASHINGTON, D.C.

Perkins Coie
attorneys at law

CONTACT: 800.586.8441 Perkins Coie LLP ATTORNEY ADVERTISING

www.perkinscoie.com

Case-closing checklist

1. Confirm that the case discovery is not covered under another legal hold.
2. Release case-specific legal holds for internal records management/IT purposes. For example:
   a. original records being used by business units,
   b. copies of records held in legal hold system if preserved by copying, and
   c. internal review databases.
3. Request certified return or destruction of copies of corporate documents and data and return of any media held by:
   a. outside counsel,
   b. forensic consultants,
   c. ediscovery processing companies,
   d. review hosting providers,
   e. testifying or consulting experts,
   f. opposing parties,
   g. courts, and
   h. referees or special masters.
4. Return or destroy any data, documents or media produced by other parties as required by agreements or court orders, including those held by:
   a. the corporation,
   b. outside counsel,
   c. forensic consultants,
   d. ediscovery processing companies,
   e. review hosting providers, and
   f. testifying or consulting experts.
5. Compare description of data or documents returned or destroyed with inventories of data or documents provided to the law firm or third party.
6. As appropriate, authorize final payment for law firms and others that submit satisfactory certificates of destruction and non-breach.
7. Continue reporting on open case closing obligations until all obligations are satisfied.
8. Update internal evaluations of law firms and vendors to indicate promptness and completeness in satisfying case closing obligations.
9. Periodically report case-closing metrics to legal and corporate management (e.g., volumes of data recovered or destroyed, cycle time from inception of case until all certificates received).

entrusting documents and data to third parties. Store the information associated with this tracking process in a secure place where the appropriate personnel can access it.

While the level of detail contained in the tracking process, often just an initial inventory, will be different in different cases, tracking the documents turned over to a third party is critical.

- *The key point is that the corporation should be able to quickly identify what was turned over to other parties, even if the knowledgeable paralegal, case manager, project manager or litigation support manager resigns, retires, is fired, dies or is reassigned.* The level of detail in an inventory will reflect the type of collection and processing that has taken place to date. For example, if corporate IT copies a custodian's file shares and emails and turns the collection over to a forensics or ediscovery processing company, the inventory may just be a total number of gigabytes for specific custodians. In smaller cases, there may be document-specific indexes.

Regardless of the form, there should be a standard way of retaining these inventories that makes sense given the size of the company, the amount of its litigation and the resources available. This may mean tracking the inventoried items as assets in a matter management system, or as an extension of a legal hold system, or placing spreadsheets with the inventories in a SharePoint site used for collaborating on litigation.

Agreements with vendors should obligate them to inventory all items passed on to other entities, at the appropriate level for the processing they may have done to the data. For example, your inventory for the data associated with a specific custodian may show that you collected a 3.2GB PST file (the type of file that contains Outlook email, calendar items, action lists, etc.). The ediscovery processing company that extracts emails for a certain period and copies them to provide to a hosting company, should be able to identify the specific number of emails provided to the hosted review provider. The inventories that are derived from subsequent processing should be added to the initial inventories in whatever system is being used.

The agreement should also require third parties to certify that there were no known or suspected data breaches while the documents were entrusted to them. The third party should also agree to indemnify the corporation for the costs of any data breaches of the copies of data that the third party held. Finally, agreements

should reserve final payment for any legal, forensic or consulting services contingent upon the completion of the specified return or certified destruction policy.

There are two purposes for requesting the certification of destruction and non-data breach. One is to motivate counsel to really safeguard the documents, and the other is to motivate them to return the copies as soon as possible after the case to minimize their own liability. This gives counsel some skin in the case-closing game.

Of course, if you must produce sensitive documents to opposing parties, seek a protective order from the court that imposes similar document and data management requirements.

If, for some reason, it is not practical to prepare an inventory or keep a copy of the documents given to a third party, at a minimum, obtain receipts or acknowledgements for any documents provided to third parties. You may also conclude that there could be significant advantages to consolidating or centralizing where all of your company's documents are held by reducing the number of outside counsel you use, using a single outside counsel for ediscovery or bringing the ediscovery function in-house.

Selecting a single cloud-based review hosting vendor and requiring all outside counsel to use that vendor can also greatly reduce the challenges of securing the destruction or return of document copies at the end of a case. There is just one set of technical staff to deal with, making efficient closing much more likely. Furthermore, while it might be impossible to conduct security audits or penetration testing of multiple hosting vendors, it may be quite practical with a single vendor.

The notion of centralizing cloud-based hosting vendors can even be extended to sharing the same hosting vendor with opposing parties. One of the authors, Anne Kershaw, has done this in both civil and criminal matters, and has cut the costs associated with such functions in half. Also, the case closeout is made simpler by having just one hosting vendor to provide for. Naturally, the vendor has to be a third party, and there must be agreements in place that prevent one party from seeing the other parties' work product; however, those issues can be dealt with by having completely separate databases used by either party.

Not only is the number of vendors holding copies of the companies' documents reduced,

but other costs (e.g., exporting documents for the opposing party to then import) can also be greatly reduced with less exposure of the documents, because they don't have to be physically shipped or sent over the Internet to another vendor.

The same approach can be used anytime some third party needs to have restricted access to a subset of documents (e.g., when disclosing documents to magistrates or judges who have to conduct in-camera reviews to determine whether privilege or work product claims for certain documents are valid, or when providing experts or consultants with a discrete set of documents). The documents in question can be put in a separate review database, and the third parties can be provided with online access to them.

- *At the end of the case, follow-up. And don't pay the final bills until you are satisfied all case closing obligations are complete.* Ideally, the matter management system or process should be configured to trigger the case closeout process when the case status is changed to "closed."

Use manual or automated tickler systems to request return or destruction of documents when a case is closed. The tickler system should be tied to the bill payment system to ensure that no further

PARTY	FUNCTION	EXAMPLES OF TYPES OF COPIES
Corporation	■ Create or receive original documents or data, use for business purposes ■ Collect ■ Review ■ Produce ■ Analyze	■ Content management systems ■ Email servers ■ File shares ■ Copies of collected documents ■ Copies of documents sent to consultants, providers or counsel ■ Review databases ■ Copies of other side's produced documents
Forensic consultant	■ Collect and analyze	■ "Pristine" set of collected documents ■ Back-up copy of collected documents ■ Working copy of collected documents ■ Set of documents to be reviewed ■ Documents attached to reports or communications
Hosting provider	■ Host review set of collected documents ■ Host documents produced by other side	■ Copy of all files received from corporation or forensic consultant ■ "Native" files (e.g., Word docs, PowerPoint presentations, etc.) linked to or referenced from review platform ■ Text and metadata extracted from native files, loaded in database ■ Copy of all produced files received from opposing and third parties
Outside counsel	■ Review ■ Produce ■ Prepare witnesses ■ Briefing ■ Prepare for trial	■ Copy of all documents collected by or sent to forensic consultant ■ Subsets of review database with corresponding native files loaded on laptops or work computers ■ Paper or electronic witness binders with copies of witness-related documents ■ Printed or electronic chron binders with copies of significant documents in chronological order ■ Copies of produced documents
Opposing counsel	■ Analyze ■ Prepare witnesses ■ Briefing ■ Prepare for trial	■ Copies of produced documents ■ Review databases with html renderings, extracted full text and metadata, PDF or TIF copies linked to database ■ Printed or electronic copies for witness binders, issue binders and chron binders ■ Subsets of collections or databases loaded on laptops or work computers

Tangled up in new laws?

Don't lose momentum. Contact Littler today.

littler.com

Littler
Employment & Labor Law Solutions Worldwide

70
YEARS

Certification of destruction and non-data breach

The undersigned hereby certifies that (Organization Name) has returned or destroyed all copies of documents provided to it by Corporation X as described on the attached Receipt Acknowledgements, other than those documents as indicated in Attachment A to this certification. The undersigned further certifies that there have been no known or suspected data breaches pertaining to the documents described on the attached Receipt Acknowledgements while they were in the possession, custody or control of (Organization Name).

Organization Name

By _____
Name _____
Title _____
Date _____

STATE OF XXX
COUNTY OF XXX
[NOTARY BLOCK]

(NOTARY SEAL)
Signature of Notary Public.

_____

payments are made until the company is satisfied that there has been complete compliance with the required return or destruction certification procedure.

Because you won't pay the vendor's final bill until the case closing process is complete, in-house counsel's obligation to follow up should be de minimis. Nonetheless, keep your eye on progress through your matter management system. While much of the day-to-day work of preparing for and executing the case-closeout process should fall to outside counsel, the in-house lawyers should monitor the process, working through the case-closing checklist with outside counsel and, if necessary, other third parties.

"Aww, come on …"

A common response to a discussion of case closeout processes is: "Aww, come on … Do I really have to do all that?" As in most things, the answer is, "It depends." There will be some instances, such as patent litigation or theft of trade secret cases, where it will be obvious that all of the documents need to be locked down as much as possible. There will be other one-off litigation (e.g., an employee's pet tarantula bites a corporate visitor) where the production is small and consists entirely of benign documents that are unrelated to the company's core business and extremely unlikely to be relevant to any future litigation.

However, here are some considerations when deciding how much of an effort to mount:

- *Passwords and security measures:* Despite all training and indoctrination, some employees will write down usernames and passwords in a document or file on their computers, email systems or file shares. Whoever gathers or culls documents for review may have copies of those files and could find the relevant files by doing something as simple as performing full-text searches for terms like "password" or "username." This particular concern could lead you to put a priority on retrieving or destroying pre-review sets of documents.
- *Data aggregation.* Even though individual cases may contain relatively small amounts of data, all the data from certain classes of cases could, in the aggregate, provide insights to competitors or provide arguable support for opposing parties in litigation. For example, data gathered in employment discrimination cases could reveal the names, ages, gender, locations and emails of key employees in mission critical areas, or might be used to support arguments about expanding the scope of individual claims to class actions. However, the data cannot be aggregated if it is disposed of as individual cases close.

Completing the case closeout procedure to make sure that all unneeded copies of corporate documents — whether held by the corporation

ACC EXTRAS ON… Document management

ACC Docket

Hands On: You Can Take Charge of Litigation! Advice for the Small Law Department (Mar. 2006). *www.acc.com/docket/lit-smalllaw_mar06*

Le Document, C'est Moi: Records Retention in Europe (Feb. 2006). *www.acc.com/docket/records-eur_feb06*

QuickCounsels

Document Management, Contract Management, Records Management, and Knowledge Management Systems: What are they, What do they do, and What are the Differences? (Feb. 2013). *www.acc.com/quickcoun/doc-manage_feb13*

Legal Project Management (Jan. 2012). *www.acc.com/quickcoun/legal-project_jan12*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

or third parties — are destroyed or returned is an important task that can be made manageable by taking basic measures before, during and at the close of each case. Have a tracking system for all documents or data collected, and tie third-parties' payments and evaluations to their submission of certificates of destruction and non-breach. In the absence of a company-wide policy and procedure, each in-house attorney and outside counsel will handle her case as she sees fit, guaranteeing a lack of uniformity and almost certain problems to come. **ACC**

NOTES

1 John W. Simek and Sharon D. Nelson, "Preventing Law Firm Data Breaches," *Law Practice, ABA,* Vol 38, No. 1, (Jan-Feb, 2012), *www.americanbar.org/publications/law_practice_magazine/2012/january_february/hot-buttons.html* (last visited Oct. 8, 2012).

Resources for further reading

International Standards Organization, ISO 15489-1 Records management, Part 1, General, describes general principles of records management and notes that, "Records retention should be managed to a) meet current and future business needs by … 3) eliminating, as early as possible and in an authorized, systematic manner, records which are no longer required. …"(p. 12, Section 9.2).

John W. Simek and Sharon D. Nelson, "Preventing Law Firm Data Breaches," Law Practice, ABA, Vol 38, No. 1, (Jan/Feb, 2012). *www.americanbar.org/publications/law_practice_magazine/2012/january_february/hot-buttons.html* (last visited Oct. 8, 2012).

James L. Michalowicz and Julie Richer, "Closing Matters and Releasing Data: What Are We Afraid Of?" *Digital Discovery and Digital Evidence*, June 1, 2009. *http://michalowiczllc.com/uploads/ClosingMattersRprnt_May_2009.pdf.*

Anne Kershaw and Shannon Spangler, "Document Hoarding Redux: Law Firms, Don't Fall Prey to the Risks of Electronic Data Over-Preservation," *EDDE Journal, ABA,* pp. 18-24. Article addresses need to address data hoarding on a more general basis. *www.akershaw.com/Documents/EDDE_Journal_Article.pdf#page=18*

James Kunick and Michael Minea, "Ediscovery under HIPAA and HITECH adds wrinkles to healthcare litigation. Inside counsel should use caution when handling personal health information as part of discovery," *InsideCounsel,* Aug. 24, 2012. *www.insidecounsel.com/2012/08/24/technology-e-discovery-under-hipaa-and-hitech-adds#.UDewIvI9OKs* (last visited Oct. 8, 2012).