

Get on Track!

Document Retention and Destruction For Law Firms

Every law firm, no matter the size, should consider instituting a formal document retention and destruction (DRD) policy. Given attorneys' – and clients' – extensive use of electronic communications and document creation, the need for solid procedures has never been greater. An effective DRD policy establishes standardized practices for the consistent creation, storage, and disposal of all material and information related to client representations.

How Does a DRD Policy Help?

Good DRD policies and procedures help manage professional liability risk in several ways:

➤ *Protect Client Confidences and Preserve Client Property*

Good DRD policies take into account lawyers' ethical obligations to preserve confidentiality and protect client property by establishing specific procedure to promptly and appropriately catalogue client property and return it to the client, and to prohibit client information from being copied, distributed, produced or otherwise disseminated to someone other than the client without client authorization and consent.

➤ *Avoid Client Disputes*

Well-documented and organized case files help lawyers to respond to client inquiries more effectively, and to provide important information needed to respond to client concerns about delays in resolving matters, disputed communications, settlement discussions, billings, and more. Many client disputes can be resolved before claims develop simply by being able to readily refer to documents evidencing agreements and communications.

➤ *Preserve Evidence for Defense of Professional Liability Claims*

When professional liability claims do occur, well-documented case files are valuable to their defense, including documentary evidence of matters such as instructions given, advice rendered, and client acknowledgement of same.

Conversely, poorly maintained files can undermine a defense. Examples include cases where the lawyer is unable to provide documentary proof of having passed along a significant settlement offer to the client, who claims that they would have accepted the offer, "if they'd only known about it." Similarly, malpractice cases have been lost because of the lawyer's inability to find a copy of the client's original instructions regarding disposition of property in an estate plan, or to show what research path she followed when investigating the validity of an opponent's argument that ultimately prevailed in litigation.

➤ *Provide Reasonable Basis and Motivation for Discarding Old Files*

Scheduled file destruction pursuant to a DRD policy is reasonable and arguably educes less suspicion of sinister behavior when documents are no longer available for discovery should litigation arise later on. Unorganized, undocumented, or random file destruction, on the other hand, can raise all sorts of concerns, as recent actions involving Arthur Anderson, Microsoft, Phillip Morris and others demonstrate. Moreover, the destruction cycle of the policy can provide the impetus lawyers may not have naturally to clear their files, purge unneeded information, and more efficiently manage the historical knowledge in the firm.

➤ *Assist in Compliance with Regulatory Obligations*

Checks and balances in DRD policies help lawyers comply with their record preservation obligations, whether regulatory (such as trust account regulations) or related to litigation (such as litigation holds in professional liability cases). They also provide attorneys with the tools needed to assist their clients in complying with their own records preservation or production obligations.

What Should a DRD Policy Consist Of?

An effective DRD policy is a written statement that defines the "what," "how long," "how and where," and "by whom" of records retention and

disposal. Good policies take time and thoughtfulness to develop. They strike a balance between considering all necessary issues and being simple enough to promote consistent implementation. To get you started thinking about the process, here are several key elements to include in any DRD policy.

- ❖ *A DRD policy should be designed to deal with both paper and electronic documents.*

While the physical nature – or lack thereof—of a document should not be the sole criterion for determining how it will be handled, every DRD policy must address both physical and electronic information. Converting printed documents to digital media, storage of physical files and digital information, accessibility of each type of file, and cataloging of each type must all be considered and addressed.

- ❖ *A DRD policy should include guidance for both retention and destruction of records.*

Keeping everything forever, while appealing and seemingly most risk averse, is no policy at all. Given the explosion of electronic information, keeping every byte of information only increases the risk that you will not be able to retrieve what you want when you need it in the future. Moreover, it increases the cost of storage and retrieval to potentially prohibitive levels.

- ❖ *A DRD policy should be designed to promote consistent use.*

Possibly the most important element of any DRD policy in any firm is consistency. Specifically how long files are kept, which materials are preserved and which are immediately discarded, how they are labeled, and whether they are kept at all is arguably secondary to a process that ensures that all files and materials, regardless of their format, origin, practice area or other defining characteristic are treated in a consistent way.

- ❖ *A DRD policy must consider applicable ethics rules, jurisdictional rules, regulations and laws.*

Law firms must research and consider applicable ethics rules regarding retention requirements, court rules or other laws or regulations regarding record-keeping for financial records, including escrows, trust accounts, client

billing and engagement agreements. Policy drafters should also consider any regulations directly applicable to the client, including business reporting requirements, federal regulations and pending litigation.

- ❖ *A DRD policy should establish standardized file structure and naming conventions to ease review and retrieval of electronically stored information.*

A standardized approach facilitates file retrieval even if the creator of the information is not available. It also helps protect information from inadvertent disclosure during discovery or file transfers.

- ❖ *A DRD policy should consider computer security issues.*

When addressing electronically-stored information in a DRD policy, a firm should confer with knowledgeable consultants for direction on how best to protect files from inadvertent destruction, corruption, natural disaster, theft or other data preservation risks.

- ❖ *A DRD policy should be written and disseminated to all firm personnel.*

Written guidelines encourage consistent implementation, promote good training and institutional history, and provide good evidence of procedures should they be questioned or face discovery. The policy should specifically identify what information or material belongs to the client and what does not, which can vary from jurisdiction to jurisdiction. Clients should also receive a written description of the policy as it pertains to their records, rights and expectations.

Implement New Policy Only On New or Pending Files

Applying a new DRD policy to active and new files is relatively straightforward. Discarding files that have already been closed is a slightly different matter. This is because you likely didn't alert the client about their expected destruction or organize them according to any specific principles before storing the files. To deal with old files, it is best to implement a plan of review, sifting through stored files to find any records that must be retained for regulatory or litigation hold purposes. Once that is done, attempt to notify the client via letter or e-mail that you will destroy the files within a specified

time period and offer them an opportunity to retrieve them. Refer to the *File Closing Checklist* in CNA's Risk Management Tool Kit at <https://w3.lawyersinsurance.com/lawyersinsurance/lawyersinsurance/html/rmanagement.html> for sample language in this regard. Finally, keep an inventory of the destroyed files, noting who oversaw the destruction, your attempts to contact the client, and the date of destruction.

Conclusion

A formal document retention and destruction policy is arguably essential to managing business, disciplinary and professional liability risk in a working law practice. While it takes time and thought to produce a comprehensive and effective policy, the effort will yield substantial returns over the years. The time to "get on track", however, is now, especially in light of the increasing demands on lawyers to become familiar with and respond to the requirements of the courts regarding conduct of electronic discovery. Watch for more detailed guidance from CNA on developing a DRD policy in early 2007. In the interim, refer to these other useful resources:

- "Model Principles of Records Management" from the Delaware Bar Association, DSBA website, <http://www.dsba.org/AssocPubs/PDFs/MPRM.pdf>
- Shuh, "The Importance of Appropriate Record Retention Policies," Digital Technologies Inc. 2003, <http://www.dtiglobal.com/articles.htm>
- Nelson and Simek, "Law Firm Document Retention Policies," Law Practice Today July 2004 (includes a sample policy), <http://www.abanet.org/lpm/lpt/articles/ftr07046.html>

July 2006

By: Emily J. Eichenhorn, J.D., Risk Control Consulting Director, CNA Lawyers
Professional Liability, CNA, 333 S. Wabash, Chicago, IL 60604

The purpose of this article is to provide information, rather than advice or opinion that is accurate to the best of the author's knowledge as of the date of this article. Accordingly, this article should not be viewed as a substitute for the guidance and recommendations of a retained professional. In addition, CNA does not endorse any coverages, systems, processes or protocols addressed herein unless such coverages, systems, processes or protocols are produced or created by CNA.

To the extent this article contains any descriptions of CNA products, please note that all products may not be available in all states. Actual terms, coverages, amounts, conditions and exclusions are governed and controlled by the terms and conditions of the relevant insurance policies.

CNA is a service mark registered with the U.S. Patent and Trademark Office. Copyright © 2006 Continental Casualty Company. All rights reserved.